

10/16/00  
JC946 U.S. PTO

10-17-00

A

PATENT  
HMD2000-1-CIPA

JC920 U.S. PTO  
09/688997  
10/16/00

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Thomas N. Giaccherini, et al.

Examiner:

Serial No.:

Group Art Unit:

Title: **METHOD FOR UTILIZING  
EXCESS COMMUNICATIONS  
CAPACITY**

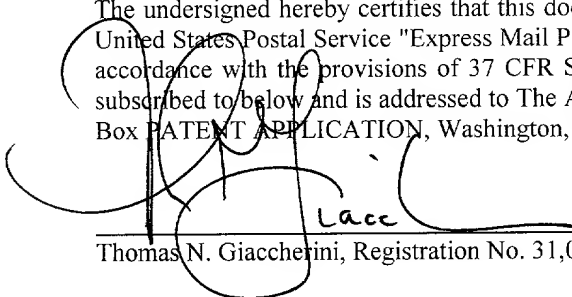
Filed: 16 October 2000

**CERTIFICATE OF MAILING BY U.S.P.S. EXPRESS MAIL**

Mailing Label Number  
EJ 789 795 241 US

Date of Deposit  
16 October 2000

The undersigned hereby certifies that this document is being deposited with the United States Postal Service "Express Mail Post Office to Addressee Service" in accordance with the provisions of 37 CFR Sections 1.53 and 1.10 on the date subscribed to below and is addressed to The Assistant Commissioner for Patents, Box PATENT APPLICATION, Washington, D.C. 20231.

  
Thomas N. Giaccherini, Registration No. 31,075

Date

16 Oct 2000

**TRANSMITTAL LETTER  
PATENT APPLICATION FILING UNDER  
37 CFR SECTIONS 1.53 & 1.10 BY U.S.P.S. EXPRESS MAIL**

The Assistant Commissioner for Patents  
Box PATENT APPLICATION  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. Sections 1.10 and 1.53, please accept the enclosed Continuation-in-Part Patent Application entitled *Method for Utilizing Excess Communications Capacity*.

09688997 1031600

This Transmittal Letter is accompanied by a Patent Application which includes:

**49** Pages of Specification plus a title page including:

**96** Claims including  
**6** Independent Claims and  
**90** Dependent Claims; and

**21** Sheets of Drawings.

No Assignments, combined Declarations & Powers of Attorney or Verified Statements of Small Entity Status are submitted at this time. No filing fee is submitted, nor is the Commissioner authorized to charge any fees to any deposit account. The Applicants intend to pay all fees connected with the filing of this Application when missing parts are submitted to the Patent Office.

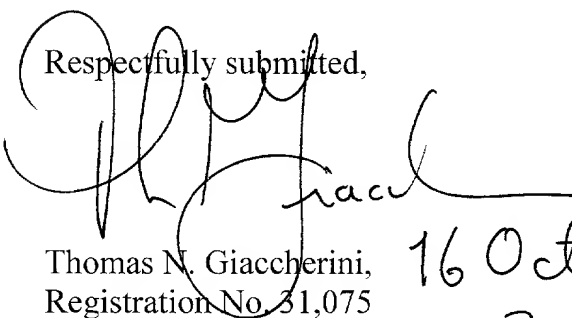
The filing fee for this Application is calculated below:

	No. Filed	Allowance	Excess	Rate	Total
Filing Fee					\$ 710
Total Claims	96	20	76	\$ 18	\$ 1368
Independent Claims	6	3	3	\$ 78	\$ 234
Multiple Dep. Claims	0	0	0	\$230	0
<b>SUBTOTAL</b>					<b>\$ 2252</b>
50% Small Entity Fee Reduction					\$ 1126
<b>TOTAL FEE</b>					<b>\$ 1126</b>

The Assistant Commissioner for Patents  
Transmission of New U.S. Patent Application  
Attorney Docket No. HMD2000-1-CIPA

Page 3

Respectfully submitted,

  
Thomas N. Giaccherini,  
Registration No. 31,075  
Attorney for Applicants

16 October  
2000.

**Anglin & Giaccherini**  
Post Office Box 1146  
Carmel Valley, California 93924

831.659.5300

Transmitted to the Patent Office by U.S.P.S. Express Mail Service,  
Label No. EJ 789 795 241 US, on 16 October 2000.

0090707 06082960

PATENT  
HMD2000-1-CIPA

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

*Application  
for  
United States Letters Patent*

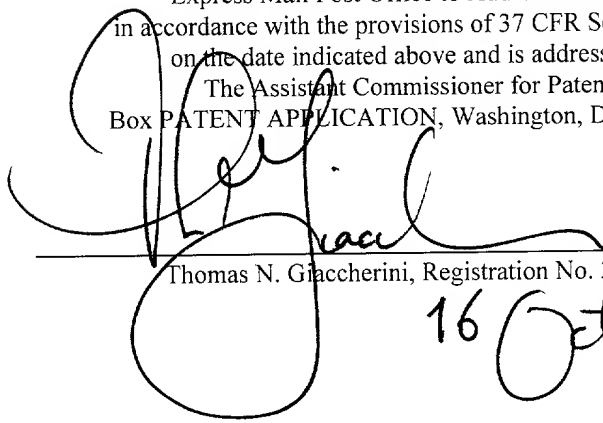
# Method for Utilizing Excess Communications Capacity

CERTIFICATE OF MAILING BY U.S.P.S. EXPRESS MAIL

Mailing Label Number  
EJ 789 795 241 US

Date of Deposit  
16 October 2000

The undersigned hereby certifies that  
this Patent Application is being deposited  
with the United States Postal Service  
"Express Mail Post Office to Addressee Service"  
in accordance with the provisions of 37 CFR Section 1.10  
on the date indicated above and is addressed to  
The Assistant Commissioner for Patents,  
Box PATENT APPLICATION, Washington, D.C. 20231.

  
\_\_\_\_\_  
Thomas N. Giaccherini, Registration No. 31,075

16 October 2000.

Inventors:  
Thomas N. Giaccherini  
James R. Stuart

009101" 26688950

# Method for Utilizing Excess Communications Capacity

## CROSS-REFERENCE TO A RELATED PENDING PATENT APPLICATION & CLAIM FOR PRIORITY

5 The present Patent Application is a Continuation-in-Part Application, which is related to pending U.S. Patent Application Serial No. 09/579,324, filed on 25 May 2000. The Applicants hereby claim the benefit of priority for any and all subject matter shared by the present Application and the pending Application filed on 25 May 2000.

## INTRODUCTION

5 The title of this Patent Application is *Method for Utilizing Excess Communications Capacity*. The Applicants, Thomas Nello Giaccherini, Post Office Box 1146, Carmel Valley, California 93924-1146, and Dr. James Riley Stuart, 1082 West Alder Street, Louisville, Colorado 80027-1046, are both citizens of the United States of America.

## FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

None.

## FIELD OF THE INVENTION

5 The present invention pertains to methods and apparatus for taking advantage of inefficiencies and excess capacities which are inherent in virtually all communications networks. More particularly, one preferred embodiment of the invention employs satellite networks to securely deliver copyrighted entertainment programming directly to homes.

## BACKGROUND OF THE INVENTION

5 In the past decade, many new satellite networks have been proposed. A few early systems, like Iridium<sup>SM</sup> and Globalstar<sup>SM</sup> have been launched, and currently provide some forms of worldwide telecommunications services. These satellites operate in low Earth orbits, and relay packets of digitized data from ground stations to customers using fixed, mobile or handheld terminals. Another satellite service called Directv<sup>SM</sup> operates in geosynchronous orbit, and furnishes a continuous stream of scheduled, analog signals that carry television programs and old motion pictures to residential customers. As of April, 2000, Directv<sup>SM</sup> had over eight million subscribers.

None of systems provides a highly interactive, high resolution entertainment digital system that supplies first-run movies on demand and protects against copyright infringement. The development of such a system would constitute a major technological advance, and would satisfy long felt needs and aspirations in the both the entertainment and telecommunications industries.

5

## SUMMARY OF THE INVENTION

The present invention provides methods and apparatus for delivering data over a network at times when the network experiences less than full transmission capacity.

5 In a preferred embodiment, a constellation of satellites in low Earth orbit receive packets of data from ground stations during these times of less than peak capacity. These packets are then conveyed to receivers over a relatively long period of time, where they are resequenced, and are then slowly accumulated on a storage device such as an array of hard drives, memory chips or other storage devices. After this  
10 “accumulation period” is completed and a full supply of data has been built up, subscribers then retrieve the data from the storage device.

The invention provides a highly secure distribution system which thwarts copyright infringement and other unauthorized copying. In one embodiment, the packets of data which are transmitted from the ground stations to the satellites, and  
15 then to the subscribers, are heavily encrypted. In one embodiment, this data is always confined to the secure network, and is never introduced to the Internet or other public networks. The data conveyed by the present invention may be video or audio programming, business data, or any other type of information. Upon arrival at the subscriber’s premises, the received signals may be decrypted, but are not capable of  
20 being copied, since the receiver does not include any external disc or tapes drives or output ports. The subscriber’s antenna, which captures the encrypted signals, may be hard-wired to the receiver. The video display which is viewed by the subscriber may



also be hard-wired to the receiver. The entire system may be shielded to mitigate any local radio frequency emissions. The system may also be tamper-proofed, so that any attempt to make unauthorized copies of data or to open the receiver cause an immediate erasure of all the data stored in the receiver.

- 5           An appreciation of the other aims and objectives of the present invention and a more complete and comprehensive understanding of this invention may be obtained by studying the following description of a preferred embodiment, and by referring to the accompanying drawings.

## A BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration which show the transfer of data from a terrestrial gateway to a low Earth orbit satellite, and then to residential and other subscribers.

5        Figure 2 is a schematic depiction of the equipment that is provided to customers including a hard-wired apparatus comprising a roof-top antenna, a set-top box and a wide-screen, flat-panel display.

10       Figure 2A is a flow diagram illustrating the steps by which a customer requests program material which is processed, sent via selected network from the source to the customer's set-top box for customer viewing.

15       Figure 3 is a schematic depiction of the *Method for Utilizing Excess Communications Capacity* of communications networks showing how programing material destined for users is interspersed with other information carried by a network.

      Figure 4 is a schematic diagram which shows how data is transferred to a user via satellite, terrestrial and wireless distribution systems.

      Figure 5 is a schematic diagram which shows further details of the data encryption systems at both the distribution data system and the customer's system.

Figure 6 presents a pictorial diagram of a tracking antenna system used by the present invention at a customer's receiving site to receive distributed data signals from a satellite or aircraft source.

Figure 7 is a pictorial diagram of a fixed antenna used by the present invention at a customer's receiving site to receive data signals from a fixed, wireless distribution source.

Figure 8 shows a schematic diagram of the principal equipment at a customer's site, a set-top box and wide screen display, and indicating the physical security employed.

Figure 9 depicts a block diagram of the set-top box, particularly showing a tamper-proof exterior box and secure input/output connections.

Figure 10 depicts principal equipment at a customer's site with no physical security, and relying therefore, on encrypted transmissions and storage end-to-end.

Figure 11 reveals in schematic form how the present invention reacts to specific customer requests by retrieving and transmitting requested data.

Figure 12 is a block diagram showing how each customer system contains layered and user-specific encryption/decryption features for the provided services of conventional digital data, video, audio, etc.

Figure 13 shows in block diagram form the multiple levels of encryption, decryption and optional security available in the instant invention.

Figure 14 is a list of functions embodied in the present invention, presented in blocks as a convenient catalogue of system server functions.

5           Figure 15 is a block diagram of the customer specific, application specific integrated circuit (ASIC) for encryption, decryption and display of data at a customer's site. It shows that no digital, decrypted data is available external to the ASIC which prevents copying the digital data.

10           Figure 16 is a block diagram of an application specific integrated circuit (ASIC) for handling service requests and responses at a customer's site.

Figure 17 is a schematic diagram illustrating the "Rainbarrel" data delivery scheme of the present invention. In this method, requested data is delivered to a customer in packets which are reassembled and "drip" into storage at the customer's site over a period of time.

15           Figure 18 is a list of steps which occur when a customer requests data from the system server.

Figure 19 is a flow diagram depicting the steps by which digital product stored at the system server is delivered through a selected network to a customer's site.

Figure 20 is a flow diagram illustrating the steps by which a user requests a system menu.

Figure 21 is a list of steps which occur when a customer requests system data from a system menu.

5           Figure 22 is a block diagram of the circuit board in the customer's set-top box illustrating the functions, inputs and outputs of the circuit board.

Figure 23 presents a partial cross-section of the exterior tamper-proof container of the set-top box, indicating a typical fastener switch which causes an erasure of all digital data stored in the box when the fastener is removed (as by tampering).

**A DETAILED DESCRIPTION OF PREFERRED  
& ALTERNATIVE EMBODIMENTS**

5 The present invention comprises methods and apparatus for delivering high quality digital signals to residential or other subscribers using the unused, excess capacity that is inherent in virtually all communication networks. In one preferred embodiment of the invention, satellites in low Earth orbit are employed to relay signals from a terrestrial gateway to subscribers in short bursts during the time that a satellite experiences underused capacity.

10 Figure 1 illustrates this particular embodiment of the present invention. A satellite SAT in Earth orbit is capable of communicating with a ground station G. The ground station G is connected to a terrestrial network, such as a public switched telephone network POTS. When a satellite SAT experiences a period of time when all its capacity is not utilized, the satellite SAT can request an upload of data from the ground station G. The ground station G then sends packets of data to the satellite SAT in short bursts. The satellite SAT is capable of delivering packets of data to many different types of terminals, including residences R, office buildings OB, cars and other vehicles C, aircraft A and boats B.

15 In another embodiment, the invention may be utilized to transmit signals S to a wide variety of terminals, including cellular phones, personal digital assistants, portable computers and displays, or other intelligent appliances.

In this embodiment, digitized, heavily-encrypted packets are beamed up to the satellite SAT from a ground station G that stores an electronic, digital copy of a copyrighted first-run motion picture. In one embodiment, the transfer of packets is accomplished using asynchronous transfer methods, and the packets are then routed to, and resequenced in order at their final destination.

Figure 2 is a schematic depiction of the equipment that is provided to the customer's site, including a hard-wired apparatus comprising a roof-top antenna ANT, a set-top box STB and a wide-screen, flat-panel display WSD. Figure 2A is a flow diagram illustrating the steps by which a customer requests program material which is processed, sent via selected network from the source to the customer's set-top box STB for customer viewing. As shown in Figure 2, the encrypted packets are received by an active beam steering antenna ANT at the subscriber's premises R, and are stored in the set-top box STB which includes a large dual-partitioned array of computer hard drives. The set-top box STB is hard-wired to the wide screen display WSD.

Figure 3 is a schematic depiction of the *Method for Utilizing Excess Communications Capacity* of communication networks showing how programing material destined for customers is interspersed with other information carried by a network. Figure 4 is a schematic diagram which shows how data is transferred to a customer via satellite, terrestrial, and wireless distribution systems. Figure 5 is a schematic diagram which shows further details of the data encryption systems at both the distribution data system and the customer's component system. Packets may be

received by the set-top box STB in very small increments over long periods of time. These incoming packets are stored in one partition 42 of the two partitions 42, 44 in the set-top box STB. The second partition 44 is used to supply on-demand unlimited-view programming while the first partition 42 is filled incrementally. In one  
5 embodiment of the invention, programming is routed to the first partition 42 over a one week period while the second partition 44 is used for viewing. At the end of the one week period, the functions of the partitions 42, 44 are exchanged. The "old" programming on the second partition 44 is then replaced with the next weeks' fare, while the current programming is viewed using the first partition 42. This "rain-  
10 barrel" method of incrementally transporting data to a large storage device enables the utilization of the under-used capacity of a satellite network.

The novel use of this method of distribution to a storage device which is securely integrated with a viewing apparatus provides secure distribution and viewing of copyrighted data. In one embodiment of the invention, the bulk of the download  
15 of programming from the satellite SAT to the set-top box STB occurs during bursts that take place at night, when normal network traffic dwindles to levels far below peak day-time usage. Figure 3 illustrates how the programming material is interspersed with gaps in network traffic.

In an embodiment which utilizes wireless networks, a roof-top receiver is  
20 installed at the subscriber's premises to capture signals broadcast from the satellites or other wireless source. In one embodiment of the invention, the receiver is coupled to a phased-array antenna which uses active beam steering to track the satellites as



they move across the sky. Figure 6 presents a pictorial diagram of a tracking antenna system 70 used by the present invention at a customer's receiving site R to receive distributed data signals S from a satellite SAT or aircraft A source.

5 Another embodiment of the invention incorporates a passive, directional or omni-directional antenna. Figure 7 is a pictorial diagram of a fixed antenna 72 used by the present invention at a customer's receiving site R to receive data signals S from a fixed, wireless distribution source G.

Figure 8 shows a schematic diagram of the principal equipment at a customer's site: antenna ANT, set-top box STB and wide screen display WSD. It indicates the physical security employed in one embodiment. Figure 9 depicts a block diagram of the set-top box STB, particularly showing a tamper-proof exterior box and secure input/output connections 80, 82. Figure 10 depicts principal equipment at a customer's site with no physical security, which relies therefore, on encrypted transmissions and storage end-to-end. The antenna ANT is hard-wired to the set-top box STB which functions as both a receiver, decryption device and storage system. The set-top box STB contains an array of computer hard drives configured in two partitions 42, 44 for storing data. In an early embodiment of the invention, the hard drive array will have a capacity of about 100 to 200 Gb. The set-top box STB, in turn, is hard-wired to a large, high-resolution flat screen WSD that is configured in a motion picture aspect ratio. The flat screen WSD may incorporate home-theater quality speakers. Table 1 below presents the attributes and operation of physical security of the data sent to the set-top box STB.

Table 1. Tamper-Proof Attributes and Operation of Set-Top Box Physical Security

Attributes: (1) Special "secure" connections between the inputs and outputs to the set-top box. (2) Access to internal circuitry of the set-top box is prevented by unique screw switches on closure and panel retention fasteners.		
Action/Component	STB Power "ON"	STB Power "OFF"
Connector removed or fasteners removed from STB access panels	Immediate "erase" signal sent to all program storage systems.	Non-alterable "erase" signal stored in non-volatile memory. All storage systems erase immediately when power returns.

The set-top box STB has no external ports, jacks, floppy-disc, tape or CD drives. All the cables 82 between the antenna, the set-top box, wide screen display and speakers are hard-wired, heavily shielded and tamper-proofed to thwart copying or piracy of the programs. The receiver is "booby-trapped," so that any attempt to open the box by removing screws or by cutting a hole to attempt to make unauthorized copies triggers the immediate erasure of all data from the hard drives, incapacitates

the set-top box and may be capable of reporting the tampering to the program provider over an Internet connection. Table 2 below lists several system security options.

Table 2. System Security Options

Physical System Protection with no Encryption	Secure network. Tamper proof equipment on customer premises. Tamper proof connections between all customer equipment components.
Physical System Protection with Encrypted Transmission Only	Secure or open network Tamper proof equipment on customer premises. Tamper proof connections between all customer equipment components.
Encryption Protection End-to-End	Open Network. Common commercial components System unique encryption: encrypted transmissions; encrypted storage; final decryption inside customers wide-screen display.

Figure 12 is a block diagram showing how each customer system contains layered and user-specific encryption/decryption features for the provided services of conventional digital data, video, audio, etc. Figure 13 shows in block diagram form the multiple levels of encryption, decryption and optional security available in the instant invention.

Figure 11 reveals in schematic form how the present invention reacts to specific customer requests by retrieving and transmitting requested data. Unlike present entertainment services like Directv<sup>SM</sup>, Home Box Office<sup>SM</sup>, Showtime<sup>SM</sup>, The Movie Channel<sup>SM</sup>, Cinemax<sup>SM</sup> or Starz<sup>SM</sup>, one embodiment of the present invention provides immediate, on-demand programming which may be viewed an unlimited number of times at the subscriber's convenience for a monthly fee. In a preferred embodiment of the invention, the programming package includes first-run theatrical releases, which has previously been shunned by the established motion picture industry due to copyright security and piracy issues. The monthly programming may also include interactive games, sports, news, educational content, classic films and both current and vintage television selections.

While the preferred embodiment of the invention is specifically configured for providing revolutionary entertainment programming, the invention may be utilized to transport any kind of data during the non-peak hours or under-utilized periods of operation of a satellite network. While the preferred embodiment is described as a particular use of low Earth orbit satellite constellations, any combination of LEO, MEO, GEO or other satellites, sub-orbital platforms or any other vehicle may be employed to implement the invention. The invention is not limited to using the excess capacity of satellite systems. Due to the novel incorporation of the "rain-barrel" feature for accumulating data slowly, over a long period of time and in small increments, any network of conventional copper land-lines, fibers, broadcast or microwave towers, cellular, PCS or any other network may benefit from a combination with the present invention. The invention may be practiced using the

Internet and TCP/IP or TCP/UDP, over public switched telephone networks or over a private data network.

5 Figure 14 is a list of functions embodied in the present invention, presented in blocks as a convenient catalogue of system server functions.

Figure 15 is a block diagram of the customer specific, application specific integrated circuit (ASIC) for encryption, decryption and display of data at a customer's site which shows that no digital, decrypted data is available external to the ASIC which prevents copying the digital data.

10 Figure 16 is a block diagram of an application specific integrated circuit (ASIC) for handling service requests and responses at a customer's site.

Figure 17 is a schematic diagram illustrating the "Rainbarrel" data delivery scheme of the present invention. In this method, requested data is delivered to a customer in packets which are reassembled and "drip" into storage at the customer's site over a period of time. Figure 18 is a list of steps which occur when a customer requests data from the system server. Figure 19 is a flow diagram depicting the steps by which digital product stored at the system server is delivered through a selected network to a customer's site. Figure 20 is a flow diagram illustrating the steps by which a user requests a system menu. Figure 21 is a list of steps which occur when a customer requests system data from a system menu.

15

20

Figure 22 is a block diagram of the circuit board in the customer's set-top box illustrating the functions, inputs and outputs of the circuit board.

Figure 23 presents a partial cross-section of the exterior tamper-proof container of the set-top box, indicating a typical fastener switch which causes an erasure of all digital data stored in the box when the fastener is removed (as by tampering).

5

003107 " 4688960

## CONCLUSION

Although the present invention has been described in detail with reference to one or more preferred embodiments, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the Claims that follow. The various alternatives for providing a highly secure data distribution system that have been disclosed above are intended to educate the reader about preferred embodiments of the invention, and are not intended to constrain the limits of the invention or the scope of Claims. The List of Reference Characters which follow is intended to provide the reader with a convenient means of identifying elements of the invention in the Specification and Drawings. This list is not intended to delineate or narrow the scope of the Claims.

## LIST OF REFERENCE CHARACTERS

A	Aircraft
ANT	Antenna
B	Boat
C	Car
DSL	Direct subscriber link to a network
G	Ground station
IC	Interactive controller
OB	Office building
POTS	Public telephone service
R	Residence
S	Wireless signals
t	Time related to satellite orbital position
SAT	Satellite
STB	Set-top box
WSD	Wide screen display



- 10 Data stream in a fully utilized network data channel
- 12 Data stream in a partially utilized network data channel
- 14 Program material provided by the present invention and inserted  
in a partially utilized network data channel
- 20 Data transfer to customer by satellite, terrestrial and wireless systems
- 22 Satellite
- 24 Satellite distribution system to system server
- 26 System server
- 28 Data system; interactive or origin
- 30 Data encryption/decryption functions
- 32 Wireless distribution system (WDS)
- 34 Satellite distribution system to customers
- 36 Terrestrial distribution system (TDS)
- 38 Equipment at customer's site
- 40 Customer's wide screen display
- 42 Low rate, secure data accumulator
- 44 Real-time playback from storage to display screen
- 50 Customer's encrypted data storage
- 52 Customer's data encryption/decryption functions
- 54 Customer's input/output and display functions
- 56 System server data encryption/decryption functions
- 58 System server data control
- 60 System server data repository
- 70 Customer's steerable or "tracking" antenna

22

## CLAIMS

What is claimed is:

1. A method comprising the steps of:

utilizing the excess capacity of a network by conveying data over said network during a period of less than maximum usage;

- 5 receiving said data during said period of less than maximum usage;

accumulating said data over an extended period of time; and

retrieving said data for on-demand use at a time after said extended period of time.

2. A method as recited in Claim 1, in which said network includes a satellite.

3. A method as recited in Claim 2, in which said satellites operate in low Earth orbit.

4. A method as recited in Claim 2, in which said satellites operate in medium Earth orbit.
5. A method as recited in Claim 2, in which said satellites operate in high Earth orbit.
6. A method as recited in Claim 2, in which said satellites operate in geosynchronous Earth orbit.
7. A method as recited in Claim 2, in which said satellites operate in mid Earth orbit.
8. A method as recited in Claim 2, in which said network includes a sub-orbital platform.
9. A method as recited in Claim 2, in which said network includes a terrestrial wired network.

10. A method as recited in Claim 2, in which said network includes a terrestrial wireless network.

11. An apparatus comprising:

a gateway means for transmitting a plurality of digitized packets of data;

a relay means for receiving said plurality of digitized packets of data from said gateway means and for retransmitting during a time period when the total communications capacity of said relay means is not fully used;

a receiver means for collecting said plurality of digitized packets of data which are transmitted from said satellite means;

said receiver means including a storage means for accumulating said plurality of digitized packets of data incrementally over an extended period of time; and

retrieving and using said plurality of digitized packets of data after a generally full program has been accumulated.

12. An apparatus as claimed in Claim 11, in which said receiver means is shielded to eliminate local radio frequency transmissions that could be used to make an unauthorized copy.

13. An apparatus as claimed in Claim 11, in which said receiver means is tamper-proofed to thwart unauthorized copying.

14. An apparatus as claimed in Claim 11, in which said relay means includes a satellite.

15. An apparatus as claimed in Claim 11, in which said relay means includes a sub-orbital platform.

16. An apparatus as claimed in Claim 11, in which said relay means includes a wired terrestrial network.

17. An apparatus as claimed in Claim 11, in which said relay means includes a wireless terrestrial network.

18. An apparatus as claimed in Claim 11, in which said receiver means is located on the Earth's surface.

19. An apparatus as claimed in Claim 11, in which said receiver means is located on the Earth's surface.

20. An apparatus as claimed in Claim 11, in which said receiver means is located in a fixed terminal.

21. An apparatus as claimed in Claim 11, in which said receiver means is located in a portable terminal.

22. An apparatus as claimed in Claim 11, in which said receiver means is located in a mobile terminal.

23. An apparatus as claimed in Claim 11, in which said receiver means is located in a sub-orbital platform.

24. An apparatus as claimed in Claim 11, in which said receiver means is located in a satellite in orbit.

25. An apparatus comprising:

transmission means for transmitting digitized packets of data over a network  
means for communicating said packets of data; said data being transmitted to  
a plurality of authorized users;

5

encryption means for securing said transmitted packets of data against  
unauthorized copying;

decryption means for decoding said transmitted packets of data only by each  
one of said plurality of authorized users;

10

a secure storage means for storing said secured packets of data; and

reproduction means for reproducing and displaying information contained in  
said decoded packets of data.

26. The apparatus as claimed in Claim 25 in which said digitized packets of data  
contain proprietary information.



27. The apparatus as claimed in Claim 25 in which said decryption means is unique to each one of said authorized users.

28. The apparatus as claimed in Claim 25 in which said transmission means employs said network means during a time period when a total communications capacity of said network means is not fully utilized.

29. The apparatus as claimed in Claim 25 in which said packets of data are delivered to each one of said plurality of users in a plurality of deposits.

30. The apparatus as claimed in Claim 25 in which said transmission means is ubiquitous.

31. The apparatus as claimed in Claim 25 in which said network means is global.

32. The apparatus as claimed in Claim 25 in which said network means is scalable.

33. The apparatus as claimed in Claim 25 in which said decryption means is partitioned into a first partial decryption means and a second partial decryption means.

34. The apparatus as claimed in Claim 25 in which said storage means is partitioned into a low-data-rate data accumulator and a high-data-rate data accumulator.

35. The apparatus as claimed in Claim 25 in which said packets of data include digitized, high-definition video signals.

36. The apparatus as claimed in Claim 25 in which said packets of data include digitized audio signals.

37. The apparatus as claimed in Claim 25 in which said packets of data include digitized text data.

38. The apparatus as claimed in Claim 25 in which said reproduction means includes a high definition television means for reproducing and displaying said decoded data packets.

39. The apparatus as claimed in Claim 25 in which said reproduction means includes a computer for reproducing and displaying said decoded data packets.

40. The apparatus as claimed in Claim 25 in which said reproduction means includes an audio tape player for reproducing and displaying said decoded data packets.

41. The apparatus as claimed in Claim 25 in which said reproduction means includes a video tape player for reproducing and displaying said decoded data packets.

42. The apparatus as claimed in Claim 26 in which said proprietary information includes first-run movies.

43. The apparatus as claimed in Claim 26 in which said proprietary data includes first-released dramatic presentations.

44. The apparatus as claimed in Claim 26 in which said proprietary data includes first-released musical presentations.

45. The apparatus as claimed in Claim 26 in which said proprietary data includes first-released recordings.

46. The apparatus as claimed in Claim 26 in which said proprietary data includes first-released books.

47. The apparatus as claimed in Claim 28 in which said transmission means overlays said network means.

48. The apparatus as claimed in Claim 33 in which said first partial decryption means is disposed in said storage means.

49. The apparatus as claimed in Claim 33 in which said second partial decryption means is disposed in said reproduction means.

50. A propagated signal comprising:

a plurality of digitized packets; said packets having the capacity to carry data;

each one of said digitized packets being transported by means of a network;  
and

5 each one of said digitized packets being transported by use of an unused  
capacity of said network.

51. The propagated signal as claimed in Claim 50 in which said data includes  
digitized, high definition video signals.

52. The propagated signal as claimed in Claim 50 in which said data includes  
digitized, audio signals.

53. The propagated signal as claimed in Claim 50 in which said data includes  
digitized text data.

54. A method of transmitting secure packets of data comprising the steps of:

providing a transmission means for transmitting digitized packets of data;

securing said transmitted packets of data against unauthorized copying with an encryption means;

5 transmitting said secure, digitized packets of data to a plurality of authorized users over a network means for communicating; said transmitting taking place during a time period when a total communications capacity of said network means is not fully used;

10 providing each one of said plurality of authorized users a decryption means for decoding said transmitted, secure, digitized packets unique to each said one of said plurality of authorized users;

providing each one of said authorized users with a secure storage means for storing said secured packets of data; and

15 providing each one of said authorized users with a reproduction means for reproducing and displaying information contained in said decoded data packets.

55. The method as claimed in Claim 54 in which the step of providing each one of said plurality of authorized users a decryption means for decoding said transmitted packets unique to each individual one of said plurality of authorized users includes the step of providing each one of said authorized users with a unique said decryption means.

56. The method as claimed in Claim 54 in which the step of transmitting said secure, digitized packets of data to a plurality of authorized users over a network means for communicating includes the step of employing an unused capacity of said network means for said transmitting.

57. The method as claimed in Claim 54 in which the step of transmitting said secure, digitized packets of data to a plurality of authorized users over a network means for communicating includes the step of delivering said secure, digitized packets of data to each one of said plurality of authorized users in a plurality of deposits.

58. The method as claimed in Claim 57 in which the step of delivering said secure, digitized packets of data to each one of said plurality of authorized users in a plurality of deposits includes the step of delivering digitized first-run movies.

59. The method as claimed in Claim 57 in which the step of delivering said secure, digitized packets of data to each one of said plurality of authorized users in a plurality of deposits includes the step of delivering digitized first-released dramatic presentations.

60. The method as claimed in Claim 57 in which the step of delivering said secure, digitized packets of data to each one of said plurality of authorized users in a plurality of deposits includes the step of delivering digitized, first-released musical presentations.

61. The method as claimed in Claim 57 in which the step of delivering said secure, digitized packets of data to each one of said plurality of authorized users in a plurality of deposits includes the step of delivering digitized, first-released recordings.

62. The method as claimed in Claim 57 in which the step of delivering said secure, digitized packets of data to each one of said plurality of authorized users in a plurality of deposits includes the step of delivering digitized, first-released books.

63. The method as claimed in Claim 54 in which said transmission means is ubiquitous.



64. The method as claimed in Claim 54 in which said transmission means is global.

65. The method as claimed in Claim 54 in which said network means is scalable.

66. The method as claimed in Claim 54 in which said transmission means overlays said network means.

67. The method as claimed in Claim 54 in which the step of providing each one of said plurality of authorized users a decryption means for decoding said transmitted packets unique to each said one of said plurality of authorized users includes the step of partitioning said decryption means into a first partial decryption means and a second partial decryption means.

68. The method as claimed in Claim 54 in which the step of providing each one of said authorized users with a secure storage means for storing said secured packets of data includes the step of partitioning said storage means into a low-data-rate data accumulator and a high-data-rate data accumulator.

69. The method as claimed in Claim 54 in which the step of transmitting said secure, digitized packets of data to a plurality of authorized users includes transmitting said packets of data containing digitized, high definition video signals.

70. The method as claimed in Claim 54 in which the step of transmitting said secure, digitized packets of data to a plurality of authorized users includes the step of transmitting said packets of data containing digitized audio signals.

71. The method as claimed in Claim 54 in which the step of transmitting said secure, digitized packets of data to a plurality of authorized users includes the step of transmitting said packets of data containing digitized text strings.

72. The method as claimed in Claim 54 in which the step of providing each one of said authorized users with a reproduction means for reproducing and displaying said decoded data packets includes the step of providing said authorized users with a means for reproducing and displaying high definition television.

73. The method as claimed in Claim 54 in which the step of providing each one of said authorized users with a reproduction means for reproducing and displaying said decoded data packets includes the step of providing each one of said authorized users with a computer for reproducing and displaying said decoded data packets.

74. The method as claimed in Claim 54 in which the step of providing each one of said authorized users with a reproduction means for reproducing and displaying said decoded data packets includes the step of providing said authorized users with an audio player for reproducing and displaying said decoded data packets.

75. The method as claimed in Claim 54 in which the step of providing each one of said authorized users with a reproduction means for reproducing and displaying said decoded data packets includes the step of providing said authorized users with a video player for reproducing and displaying said decoded data packets.

76. The method as claimed in Claims 62 in which the step of providing each one of said authorized users with a reproduction means for reproducing and displaying said decoded data packets includes the step of providing said authorized users with a printer that includes a pager binder for reproducing and displaying said digitized first-run books.

77. The method as claimed in Claims 71 in which the step of providing each one of said authorized users with a reproduction means for reproducing and displaying said decoded data packets includes the step of providing said authorized users with a printer that includes a pager binder for reproducing and displaying said digitized text strings.

78. The method as claimed in Claim 55 in which the step of providing each one of said authorized users with a unique said decryption means includes the step of providing said authorized users with a first partial decryption means and a second partial decryption means.

79. The method as claimed in Claim 78 in which the step of providing said authorized users with a first partial decryption means and a second partial decryption means includes the step of disposing said first partial decryption means in said storage means.

80. The method as claimed in Claim 78 in which the step of providing said authorized users with a first partial decryption means and a second partial decryption means includes the step of disposing said second partial decryption means in said reproduction means.

81. A method of doing business comprising the steps of:

placing a plurality of digitized packets of data in a secure archive;

distributing said plurality of digitized packets of data to a customer using a  
secure digital distribution system during a time period when a total  
communications capacity of said network means is not fully used; and

said customer having the capability to reproduce and display said proprietary  
information.

82. The method as claimed in Claim 81 in which the step of placing a plurality of  
digitized packets of data in a secure archive includes the step of placing a plurality of  
digitized packets of data which contain proprietary information in said secure archive.

83. The method as claimed in Claim 82 in which the step of placing a plurality of digitized packets of data which contain proprietary information in said secure archive includes the steps of:

5           securing said digitized packets of data against unauthorized copying with an encryption means;

          transmitting said secure, digitized packets of data to said customer over a network means for communicating said digitized packets of data;

          providing said customer with a secure storage means for archiving said digitized packets of data;

10          providing said customer with a decryption means for decoding said transmitted packets; said decryption means usable *only* by said customer; and

          providing said customer with a reproduction means for reproducing and displaying information contained in said decoded data packets.

5

providing said first level of encryption with a key which is unique to said customer; and

43

85. The method as claimed in Claim 83 in which the step of providing said customer with a decryption means for decoding said transmitted packets, said decryption means usable only by said customer, includes the steps of:

5 partially decrypting said transmitted packets with a first decryption means; said first decryption means disposed in said secure storage means;

storing said partially decrypted said transmitted packets in said secure storage means until said customer is ready to access and display said packets of data; and

10 decrypting said partially decrypted transmitted packets with a second decryption means; said second decryption means disposed in said reproduction means; said second decryption means using said key which is unique to said customer.

86. The method as claimed in Claim 83 in which said transmission means is ubiquitous.

87. The method as claimed in Claim 83 in which said transmission means is global.



88. The method as claimed in Claim 83 in which said network means is scalable.

89. The method as claimed in Claim 83 in which said transmission means overlays said network means.

90. The method as claimed in Claim 83 in which the step of providing each one of said authorized users with a secure storage means for storing said secured packets of data includes the step of partitioning said storage means into a low-data-rate data accumulator and a high-data-rate data accumulator.

91. The method as claimed in Claim 83 adapted for distributing first-run movies, further comprising the step of:

delivering said secure digitized packets of data containing digitized, first-run movies to said customer in a plurality of deposits.

92. The method as claimed in Claim 83 adapted for distributing first-release musical presentations, further comprising the step of:

delivering said secure digitized packets of data containing digitized, first-released musical presentation to said customer in a plurality of deposits.

93. The method as claimed in Claim 83 adapted for distributing first-released recordings, further comprising the step of:

delivering said secure, digitized packets of data containing digitized, first-released recordings to said customer in a plurality of deposits.

94. The method as claimed in Claim 83 adapted for distributing first-released books, further comprising the step of:

delivering said secure, digitized packets of data containing digitized, first-released books to said customer in a plurality of deposits; and

5 printing on said customer's site said digitized first-released books using a printer that includes a page binder.

delivering said secure, digitized packets of data containing digitized, first-released dramatic presentations to said customer in a plurality of deposits.

delivering said secure, digitized packets of data containing digitized, first-released high definition television programs in a plurality of deposits.

# **Method for Utilizing Excess Communications Capacity**

## **ABSTRACT OF THE DISCLOSURE**

Methods and apparatus for the secure and copy-proof distribution of data are disclosed. In a preferred embodiment of the invention, a network of satellites in low Earth orbit are used to convey packets of data from ground stations to set-top boxes installed in residences. The data is conveyed from the ground stations and to the set-top boxes during times when the network capacity is not fully utilized.

5

## SEQUENCE LISTING

Not Applicable.

1/21

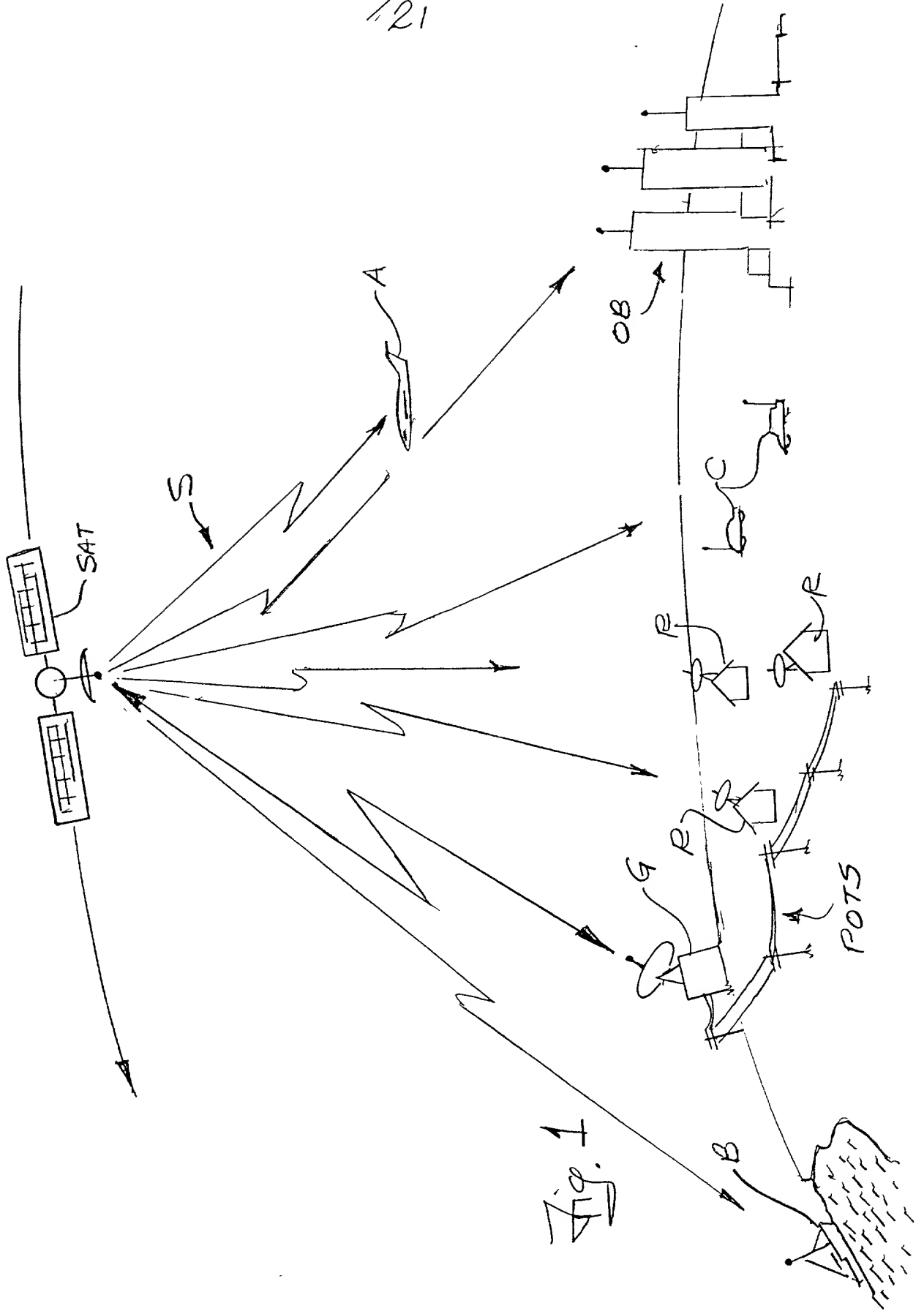
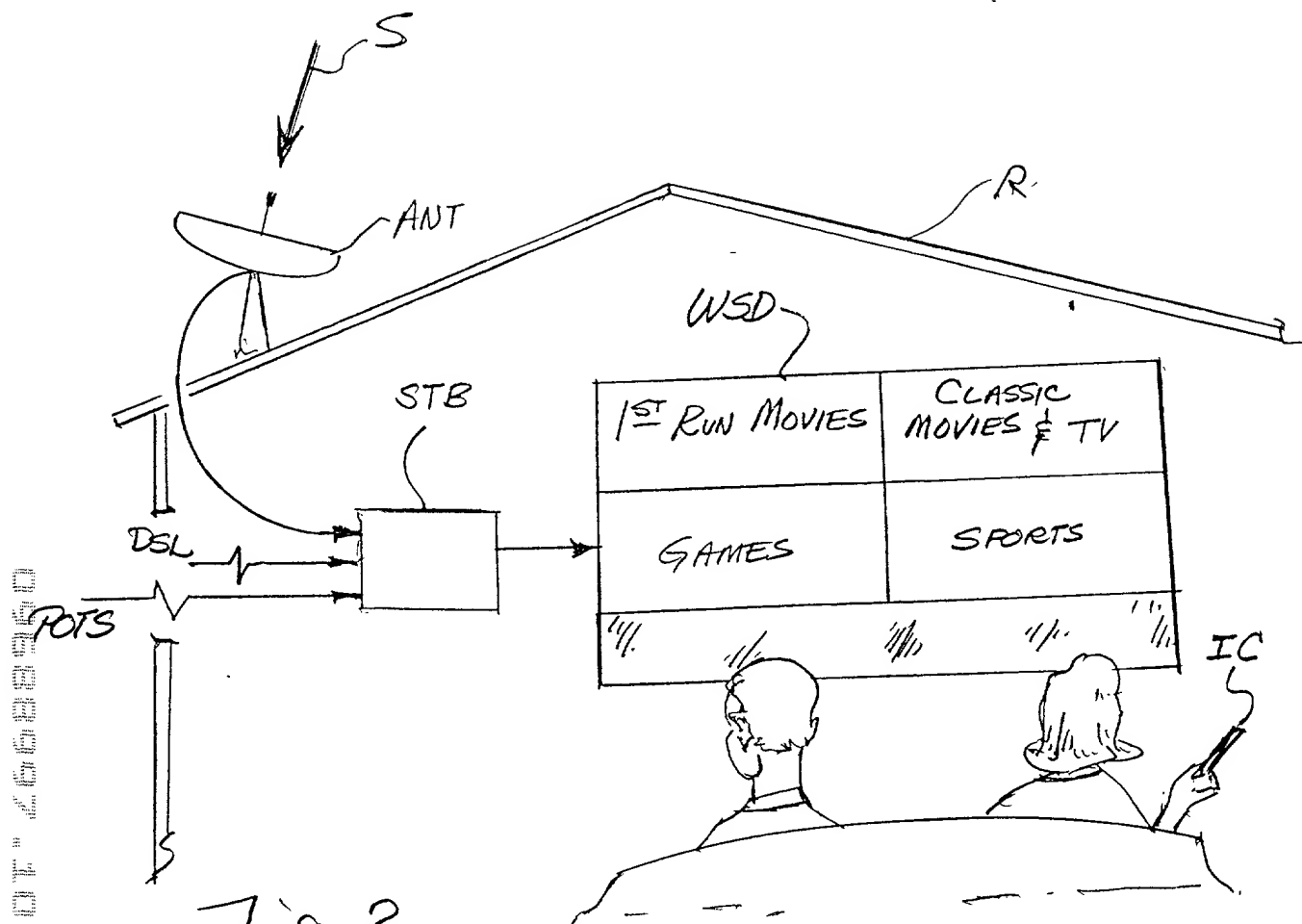


Fig. 1

2/21



3/21

Sky Vault Operation Flow Chart

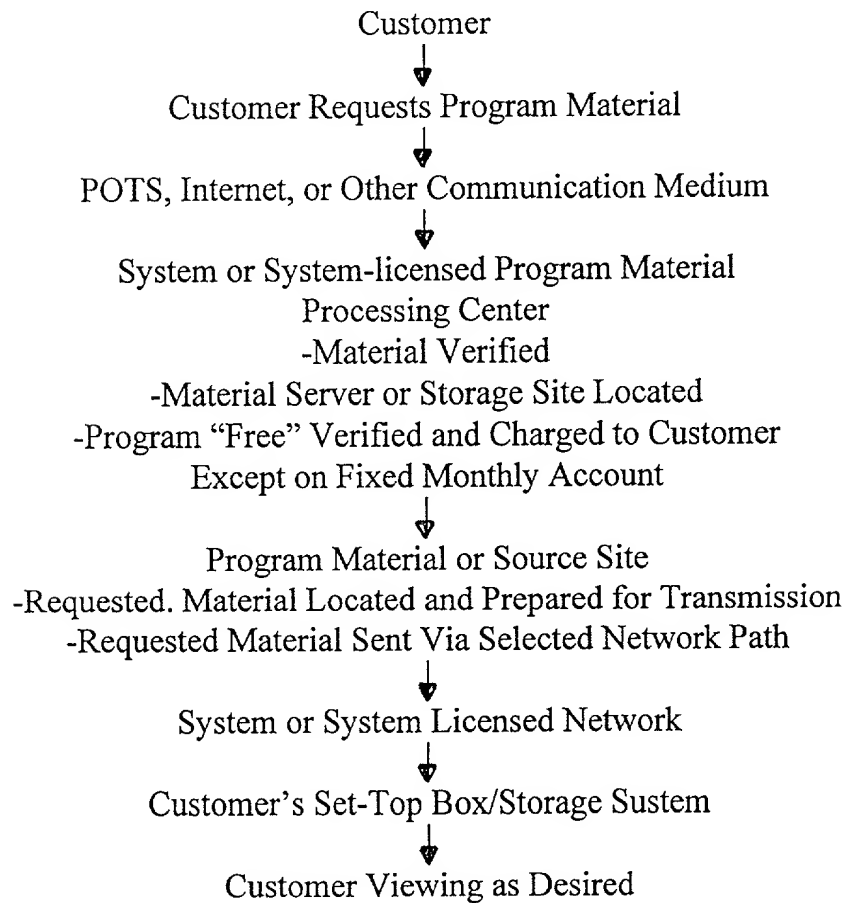


Fig. 2A



4/21

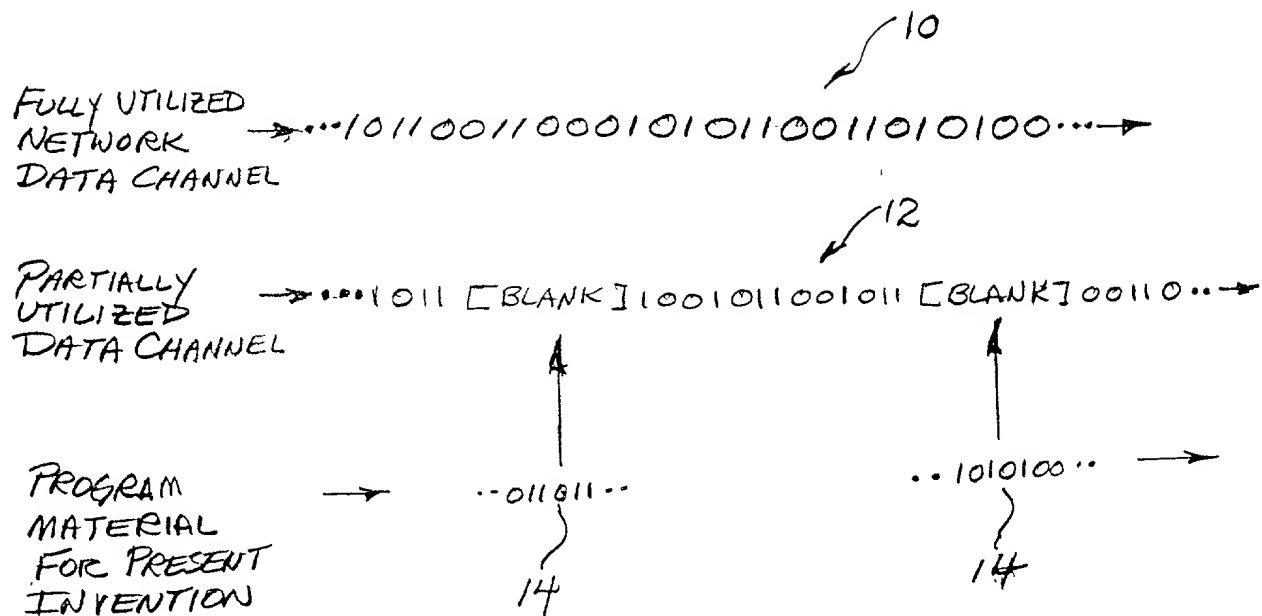


Fig. 3

00507-2682960

5/21

20

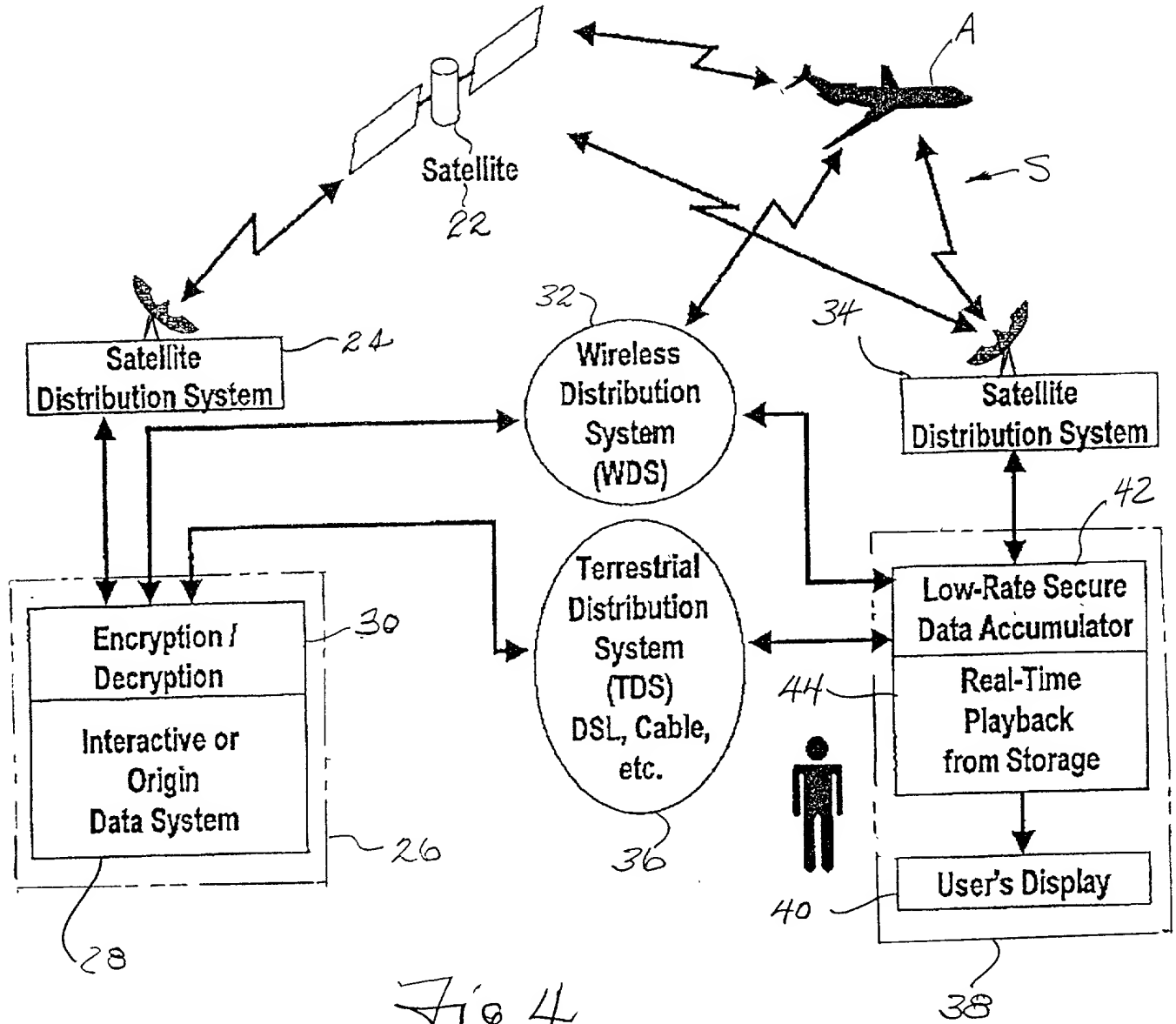


Fig. 4

009707 2688960

6/21

00507 2622560

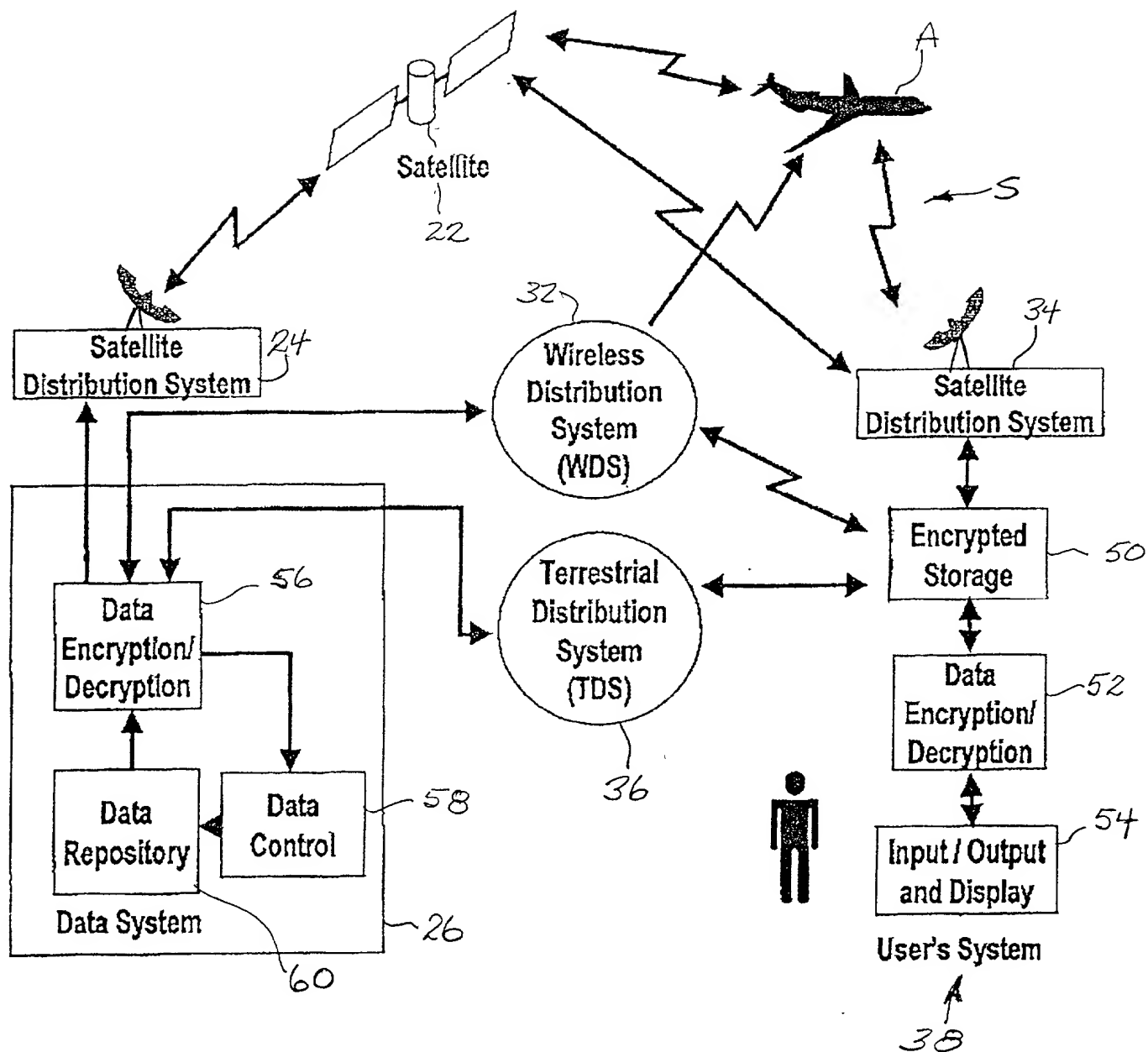
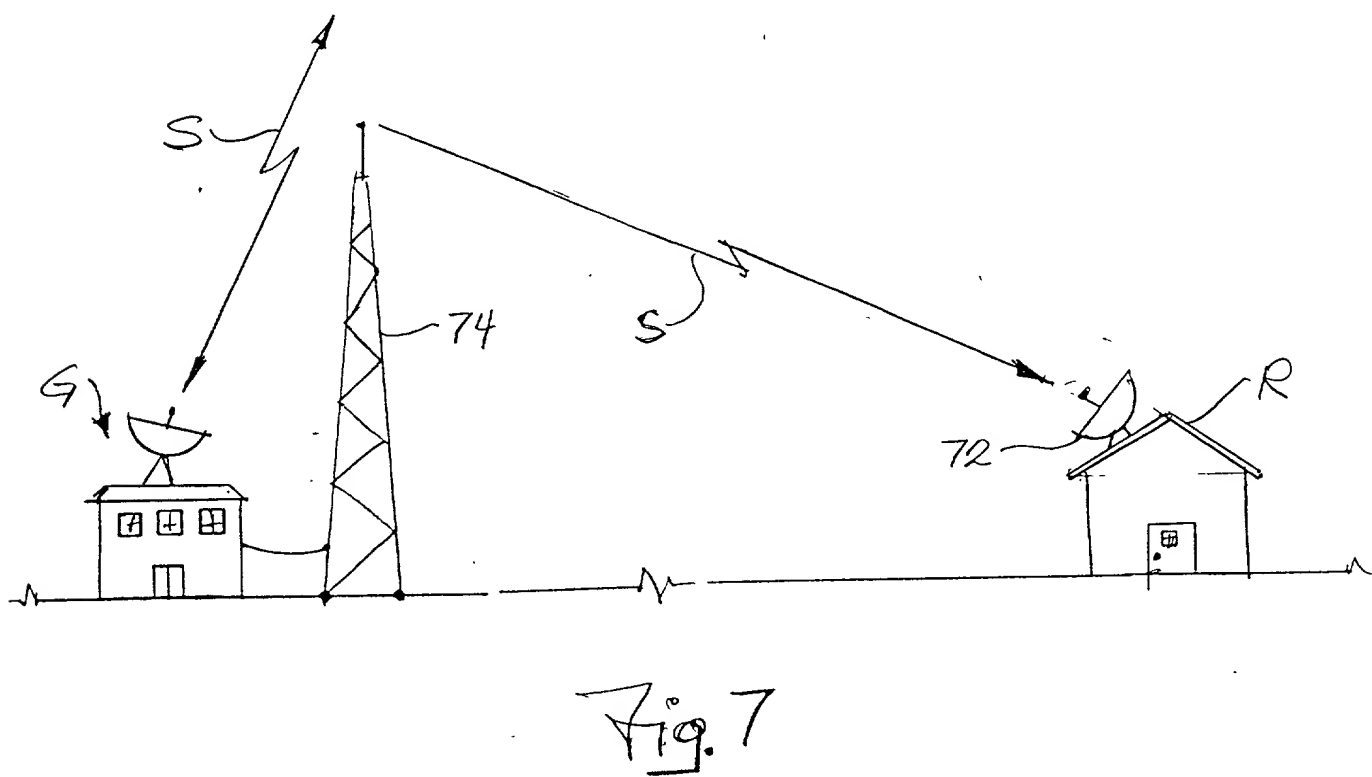
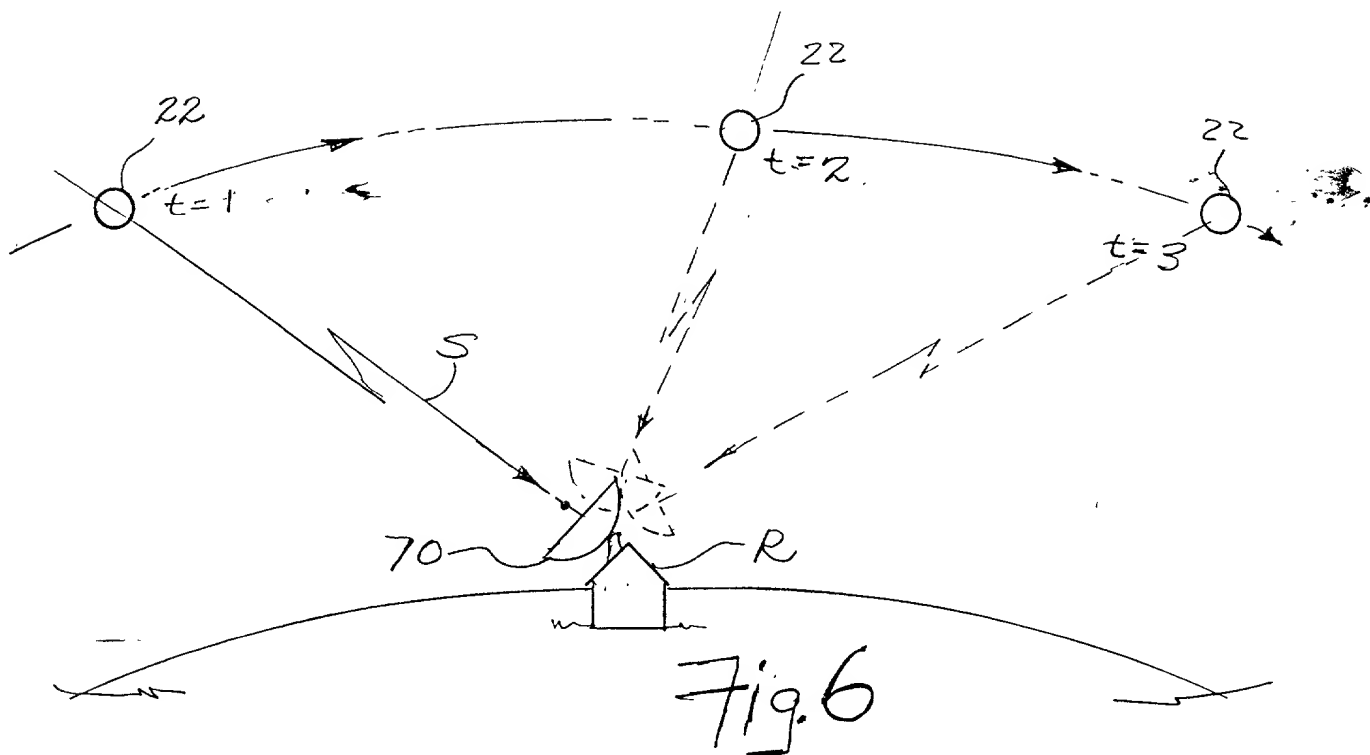


Fig. 5

7/21



8/21

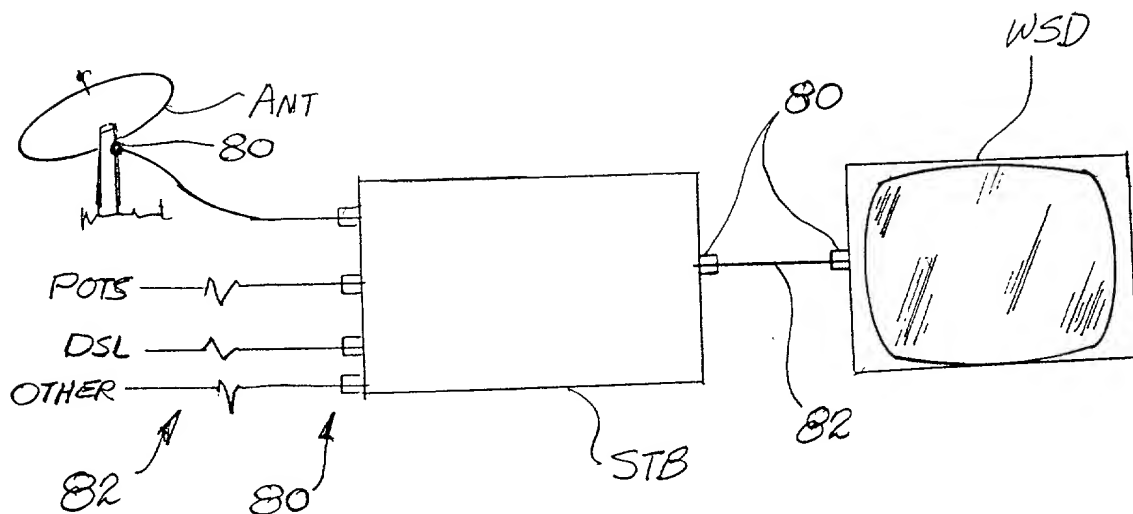


Fig. 8

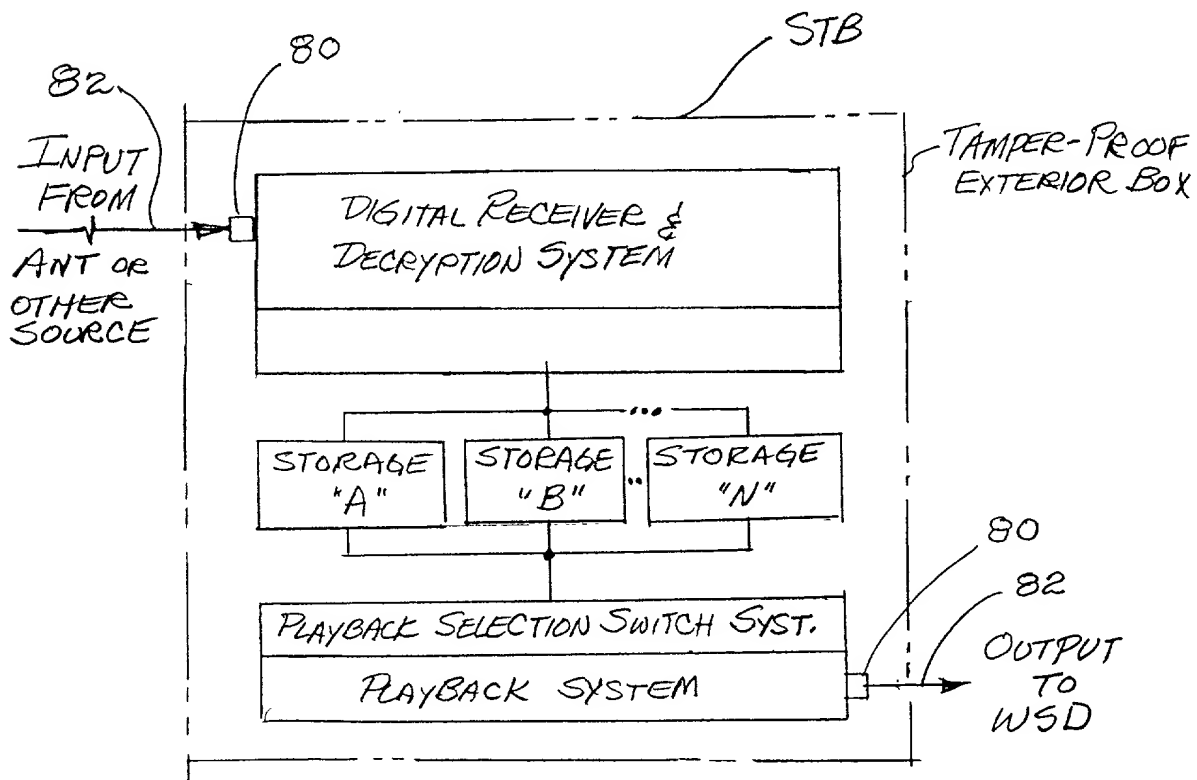


Fig 9

00907 2662960

9/21

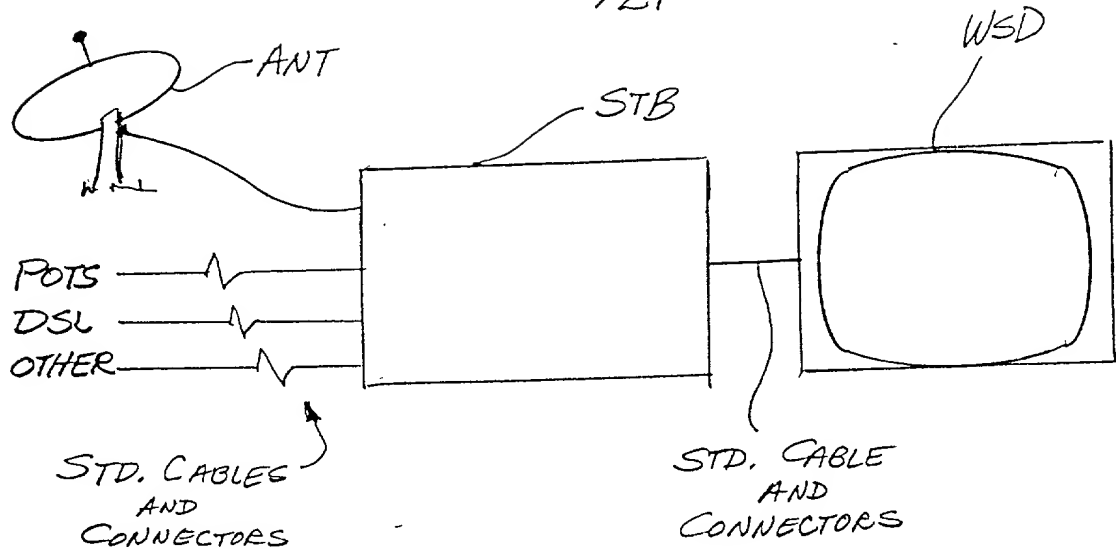


Fig 10

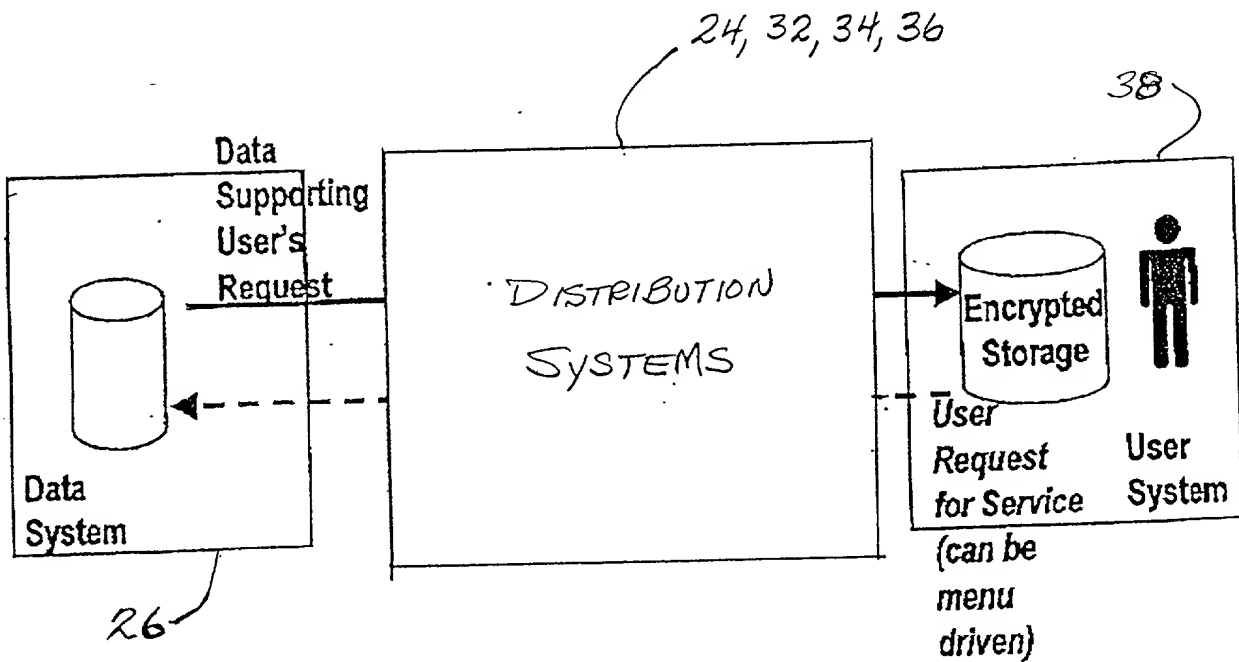


Fig. 11

DocId:32682560

10/21

Remotely Configurable  
Encryption / Decryption  
Algorithms

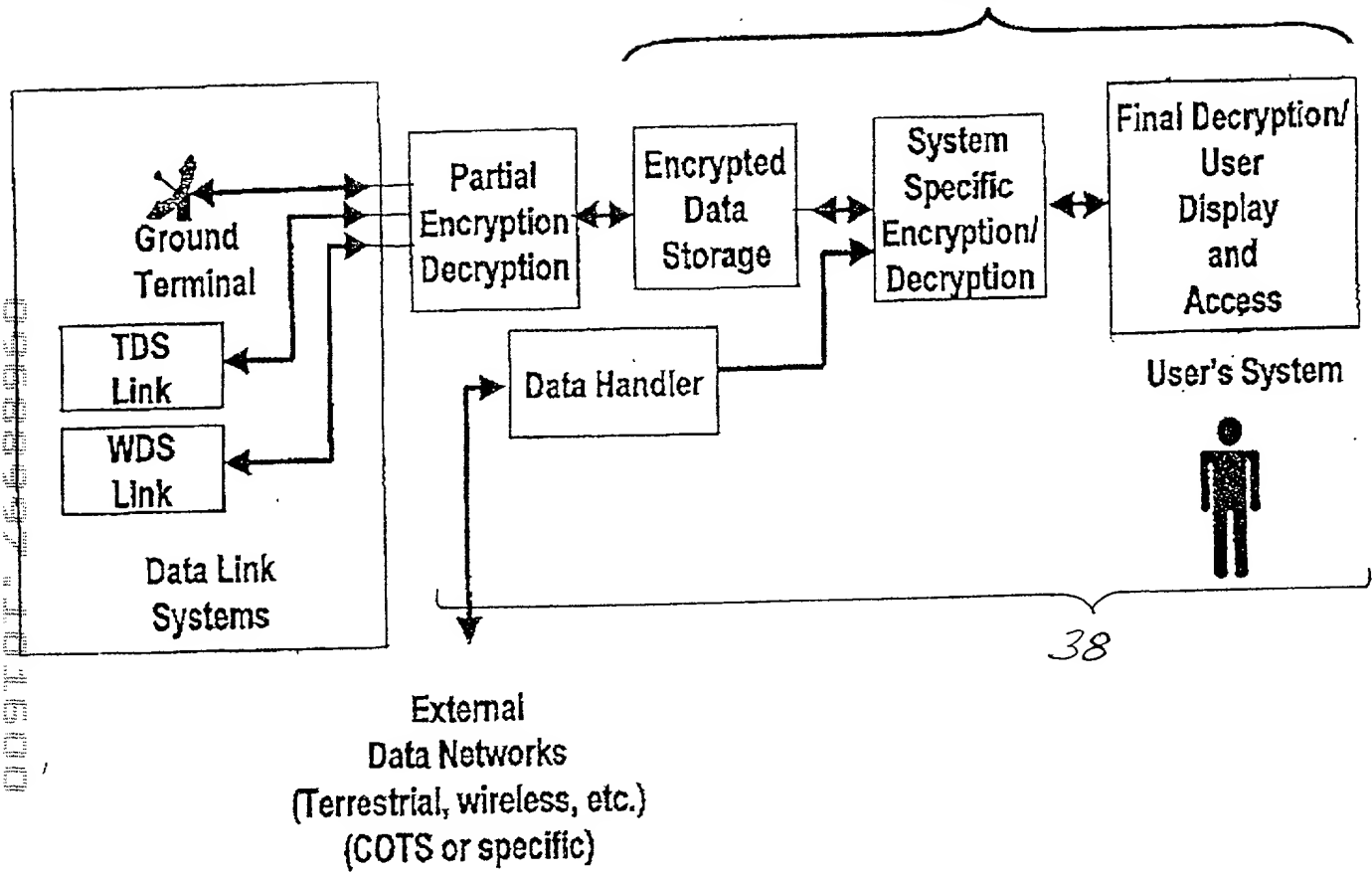


Fig 12

11/21

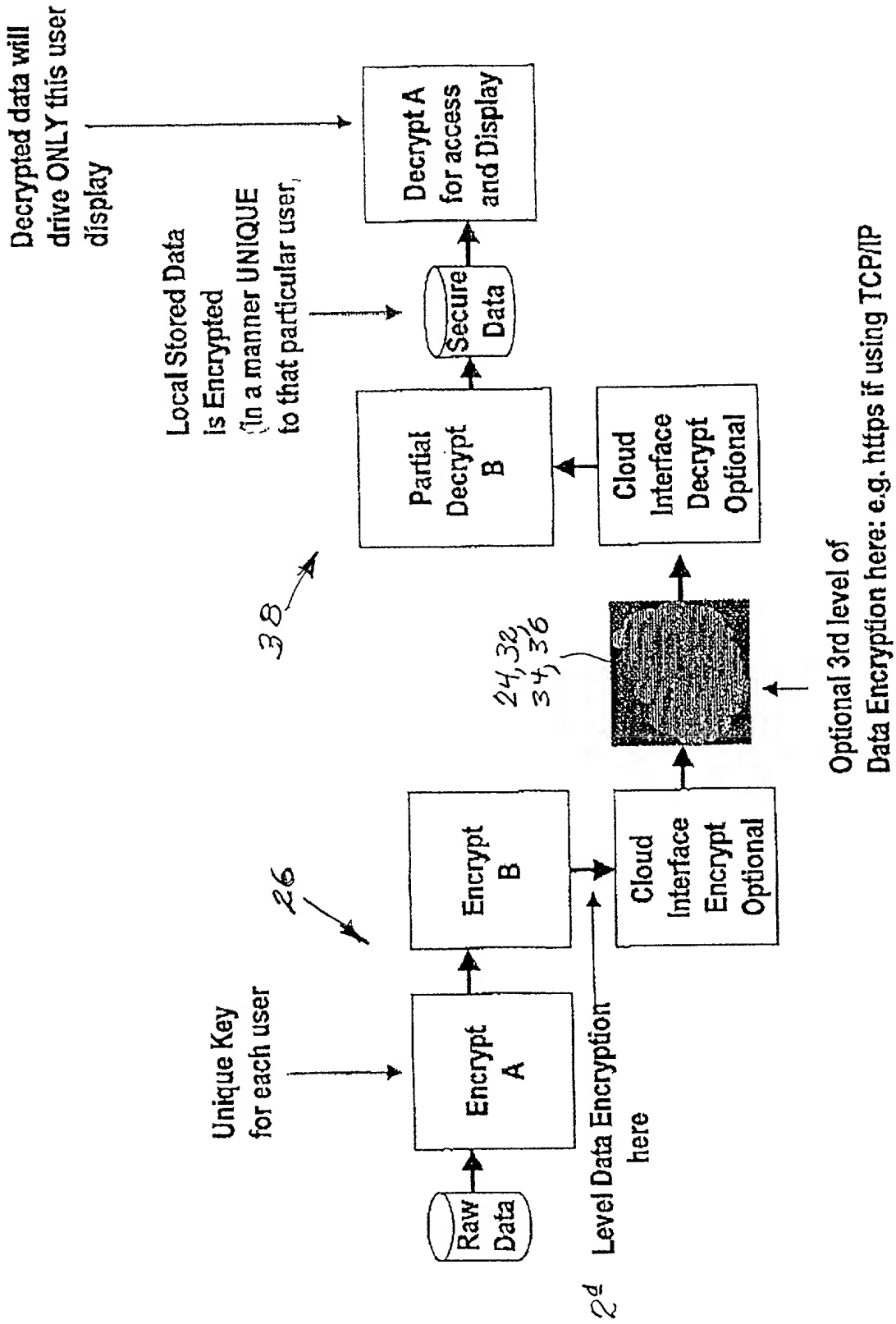


Fig. 13



[illegible]

## SYSTEM SERVER FUNCTIONS

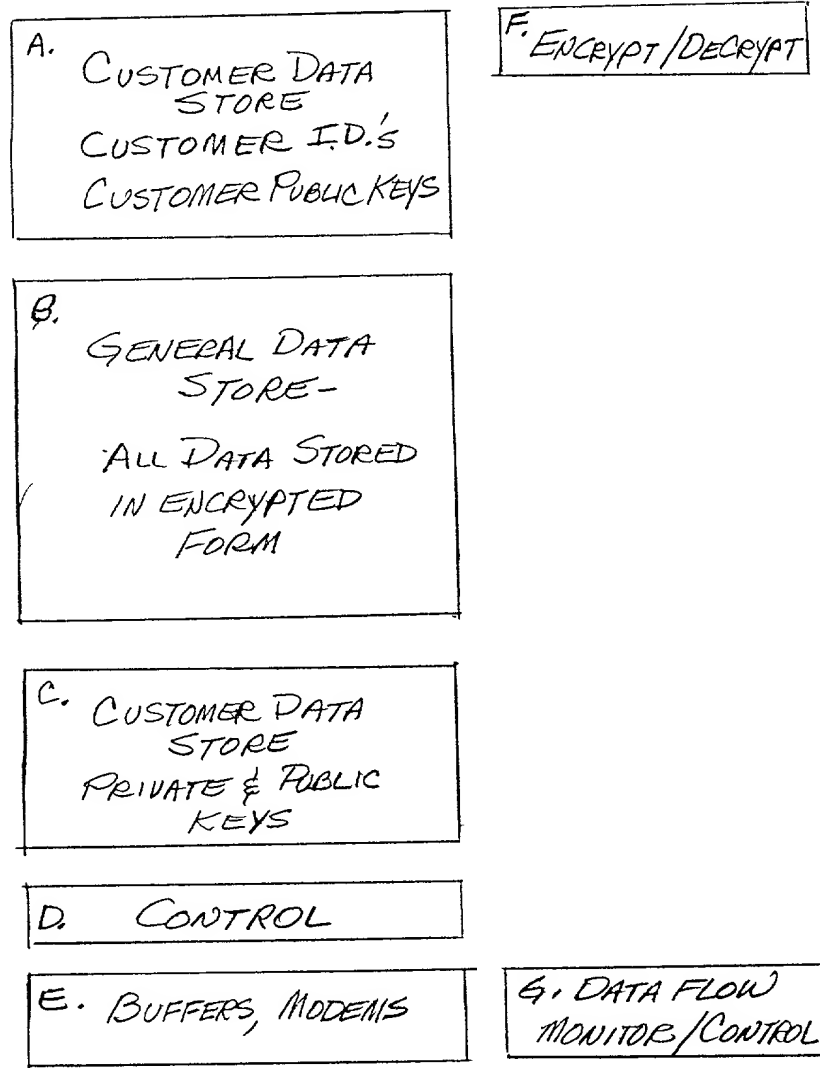
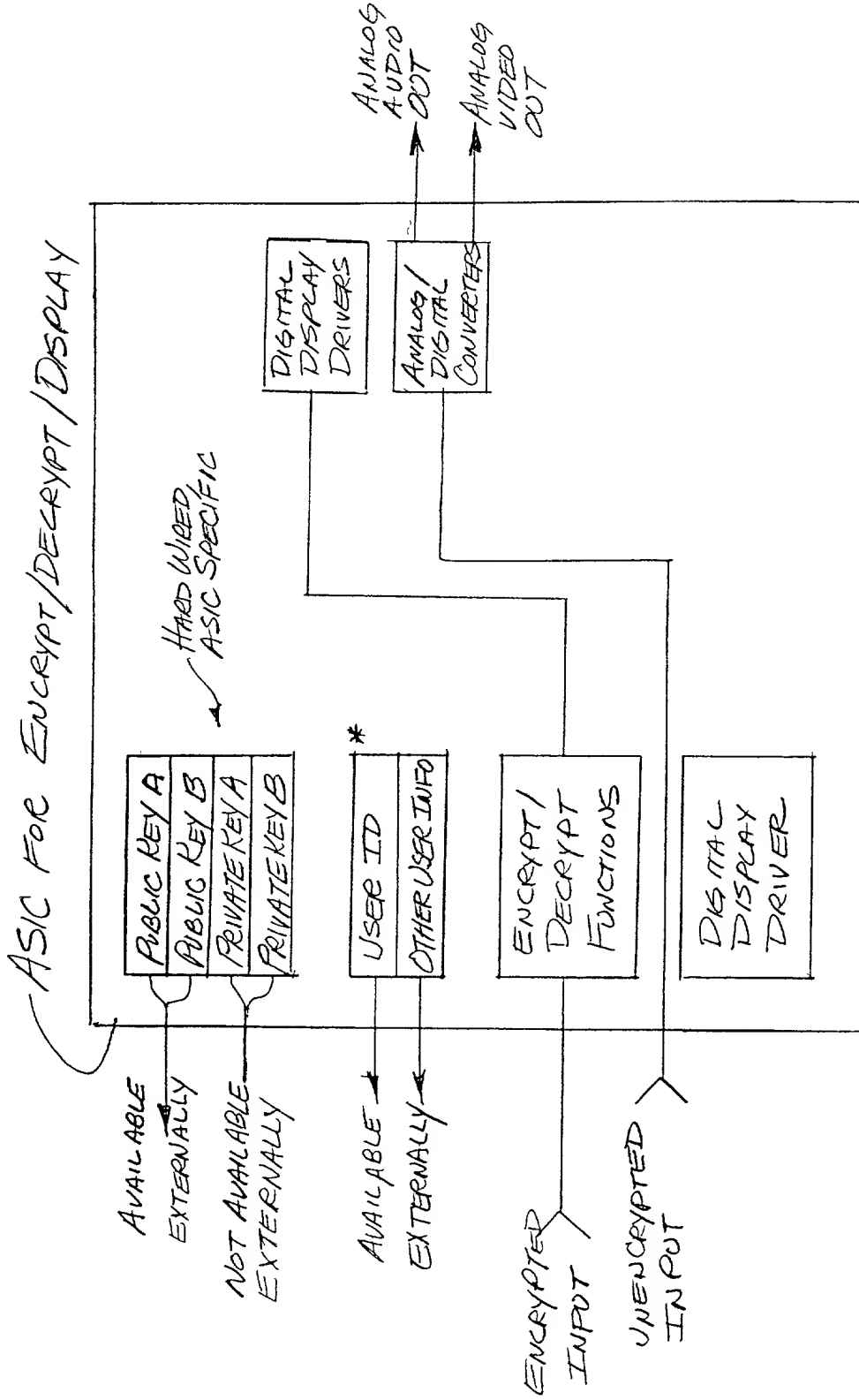


Fig. 14

13/21

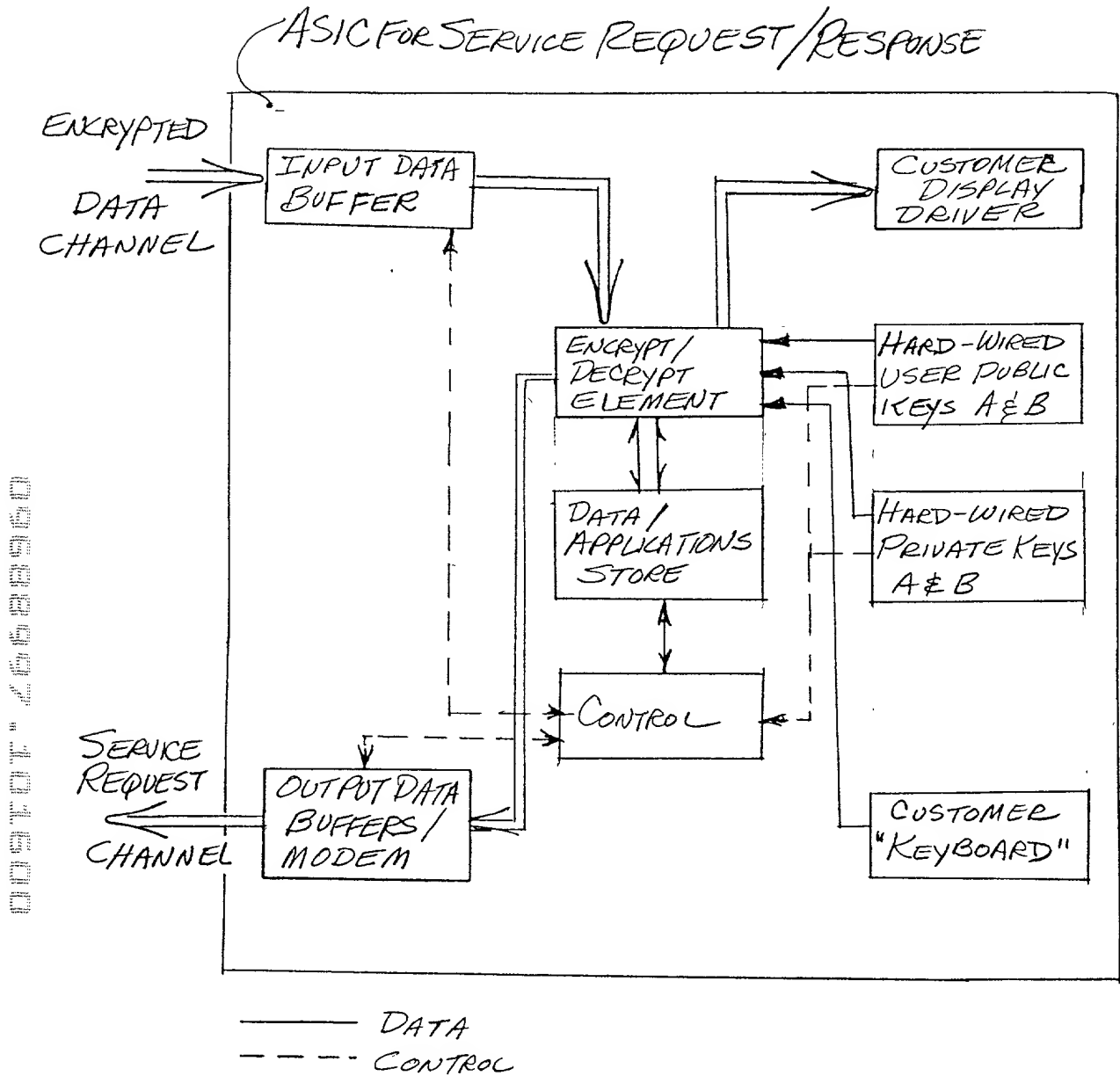


\* MAY BE STORED EXTERNALLY

NOTES: 1) CUSTOMER-SPECIFIC ASIC,  
ANALOG & DIGITAL CIRCUITS  
2) NO DIGITAL, DECRYPTED  
DATA AVAILABLE EXTERNAL  
TO ASIC

Fig. 15

14/21



- NOTES:
- 1) Request for data - CONTROL sends publicKeys A & B TO SYSTEM SOURCES via OUTPUT DATA BUFFER; Sends DATA I.D. NUMBER to identify stored data upon receipt.
  - 2) Data reception - Control identifies DATA & applies Private Keys A or B for Storage or Display.

Fig. 16

# Multiple Path "Rainbarrel" Data Delivery

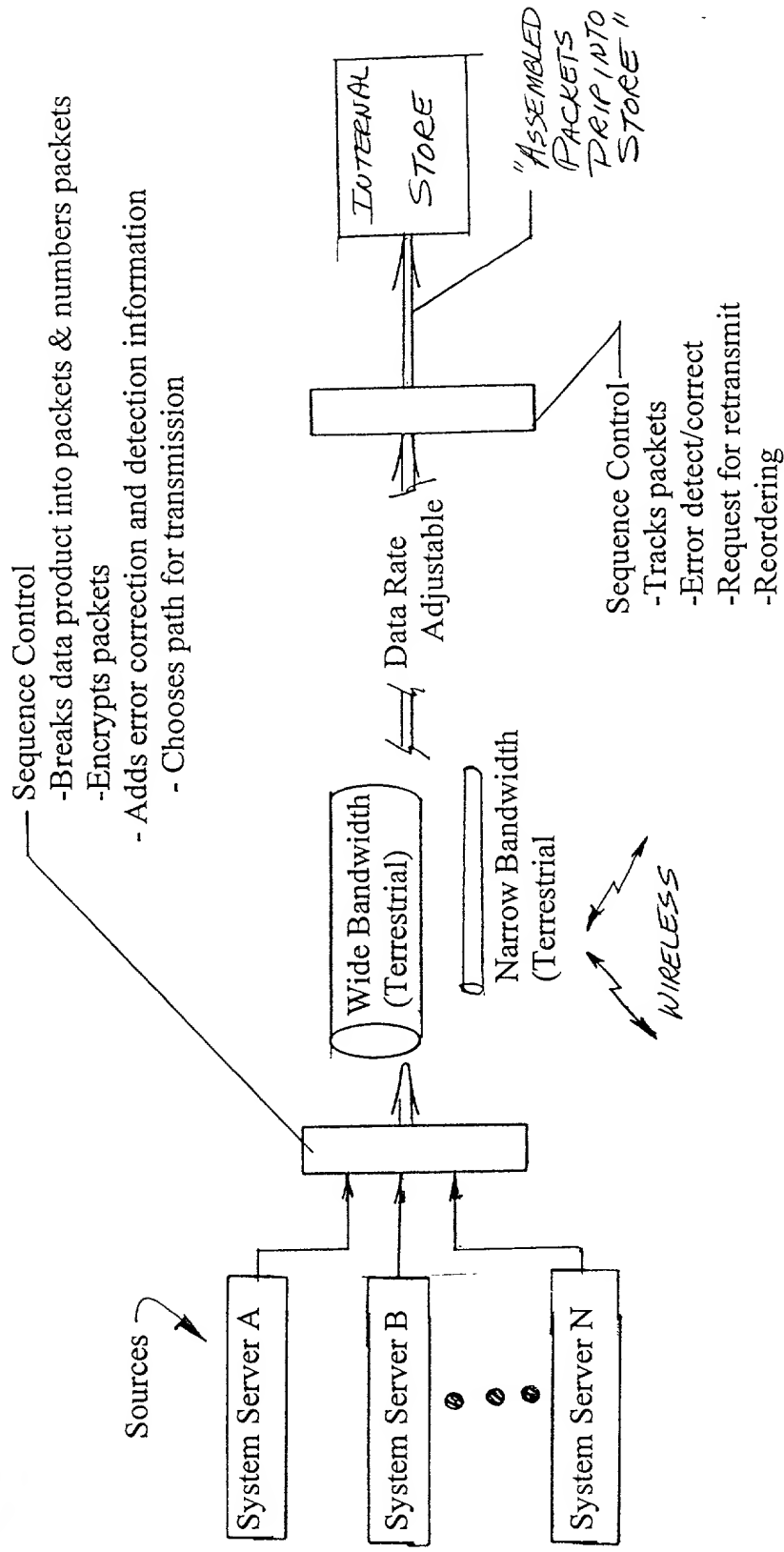


Fig.17

16/21

### Request for Data and Response

- 1) Customer requests data menu from system server.
- 2) System server responds with menu, etc.
- 3) Customer requests "data".
  - Generic request: customer sends customer ID, public key A; encrypts by public key.
  - Request for specific data: customer sends ID, public keys A and B; encrypts by public key
- 4) Network encrypts/decrypts (for example, with https); system server decrypts and searches data base for response.
- 5) System server extracts data, "packetizes" the data.
  - Server encrypts the data with public key A
  - Network encrypts/decrypts
- 6) Network operating system routes encrypted packets over available routes to customer.
- 7) Customer decrypts with private key A
  - Generic request: Display menu
  - Specific request: Data buffered, reassembled and stored in encrypted form.

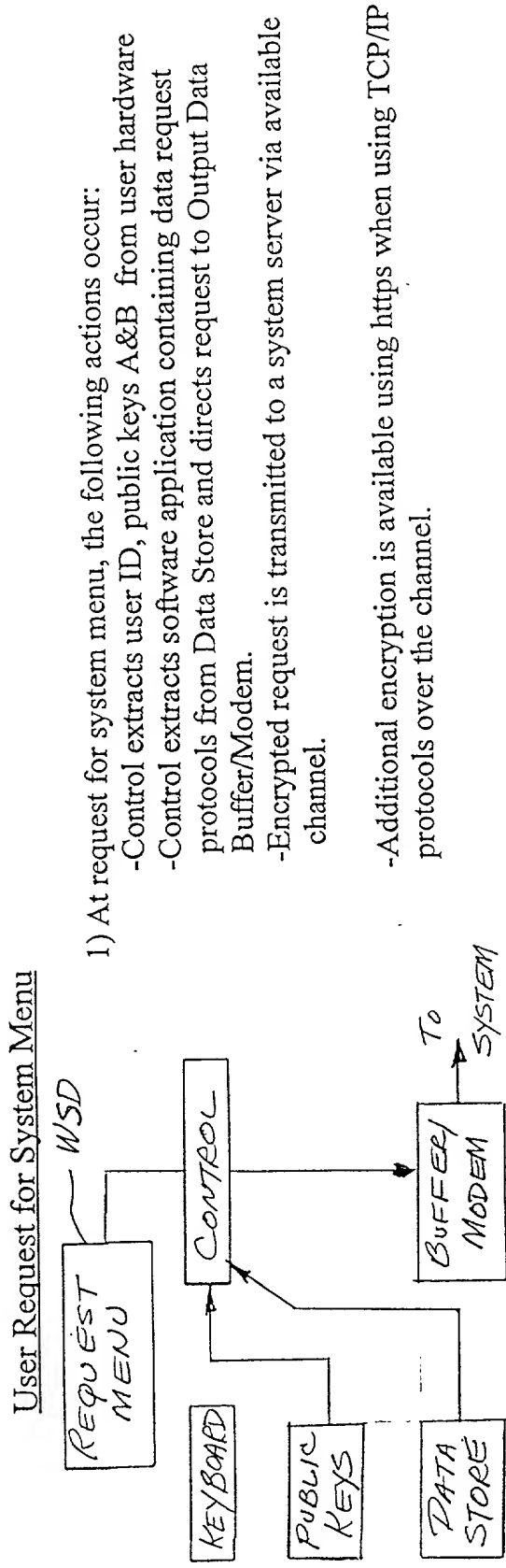
Fig. 18

Table 1. Demographic characteristics of the study population	
Age (years)	Mean (SD)
Male	55.2 (10.5)
Female	56.8 (11.2)
Marital status	
Married	78.5%
Single	21.5%
Education level	
High school or above	65.2%
Below high school	34.8%
Occupation	
Professional	12.3%
Managerial	18.7%
Technical	25.4%
Service	32.1%
Unemployed	11.5%
Income (USD/month)	
< 1000	15.2%
1000-2000	28.7%
2000-3000	35.1%
> 3000	21.0%
Health insurance	
Yes	89.3%
No	10.7%
Smoking status	
Smoker	22.5%
Non-smoker	77.5%
Alcohol consumption	
Regular	8.9%
Occasional	14.3%
Never	76.8%
Comorbidities	
Hypertension	35.2%
Diabetes	18.7%
Cholesterol	25.4%
Obesity	12.1%
Depression	9.8%
Family history of cancer	
Yes	15.6%
No	84.4%



Fig. 19

18/21



- 2) At receipt of menu data, Control decrypts with private key B and stores in Data/Application Store.
- 3) When data transfer is complete, Control causes display to indicate "Menu Available."
- 4) Customer requests menu display from the keyboard (or mouse, etc.)
- 5) Control extracts encrypted data from Store and performs second decryption using private key A.
- 6) Data is displayed on screen, but digital unencrypted form of the data is unavailable outside of display ASIC.

Fig. 20

19/21

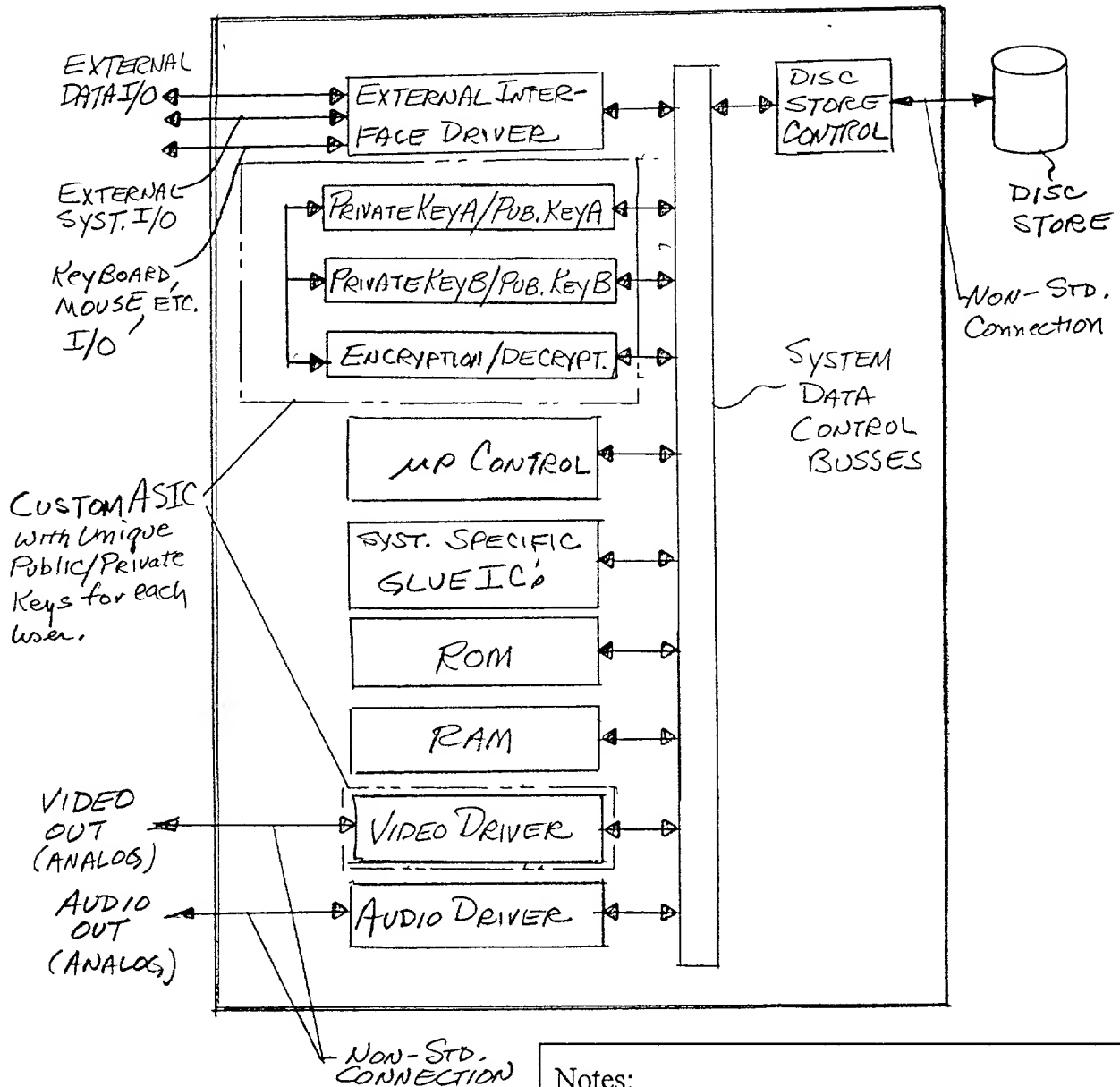
### User Request for System Data

- 1) Customer requests system menu data by keyboard (or mouse, etc.)
- 2) Request is encrypted using public key A and stored in Data/Applications Store. Customer ID,, public keys A and B are attached.
- 3) Request is also encrypted using System public key and sent to Data Flow Monitor/Control and Buffers/modems for transmission via available digital channel.
- 4) At receipt of data request by System, the following actions occur:
  - Controller stores customer request in a General Data Store.
  - Requested data is encrypted using customer public keys A & B and sent to data Flow Monitor/Control for progressive transmission through buffers/modems.
  - Selected least significant bits of data, controlled by customer public key, are altered with a **customer-specific** signature.
- 5) When customer receives data, Control decrypts data using private key B and stores data blocks in Data/Applications Store. When all data blocks are received, Control notifies user via the display.
- 6) When customer requests to view the data, Control decrypts it using private key A and removes the digital signature. Control then sends the data to the display driver.
- 7) Note that all keys are hardware specific and not available to the operating system. They are usable only by the encrypt/decrypt/display ASIC. No "Hacker" access since digital data is never available outside the user's hardware.

Fig. 21



20/21



Notes:

1. Public keys available on System Data Bus.
2. Private keys within and only available to encryption/decryption ASIC.
3. Digital data never available outside of ASIC in unencrypted form.
4. All data stored on disc, or equivalent, is in encrypted form.
5. Analog video and audio data transmitted to off-board displays via non-standard connectors and cables.

Fig. 22

21/21

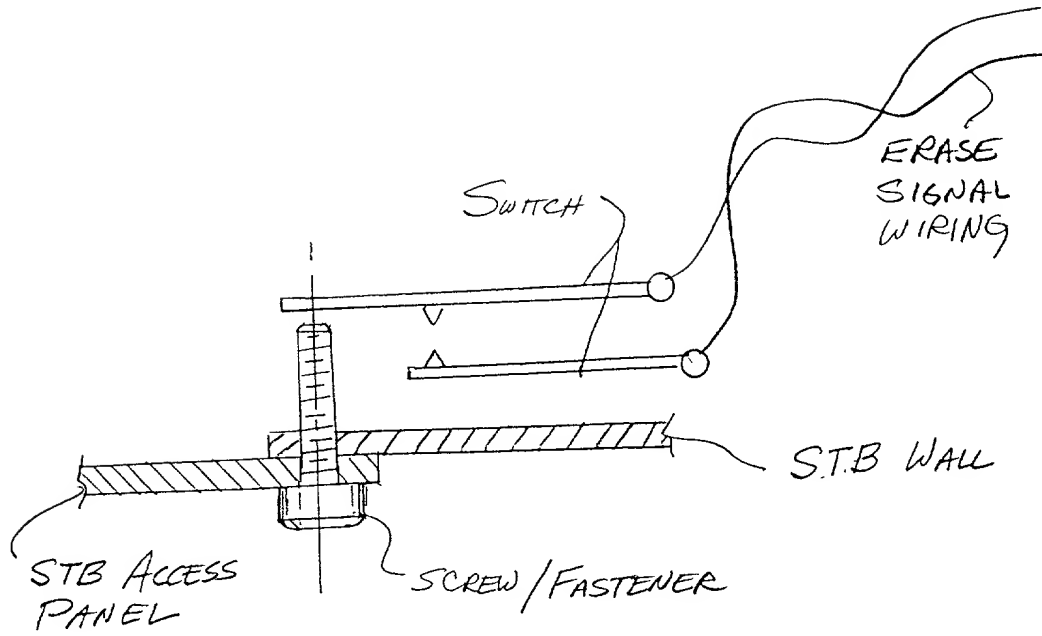


Fig. 23

009T01 25688960